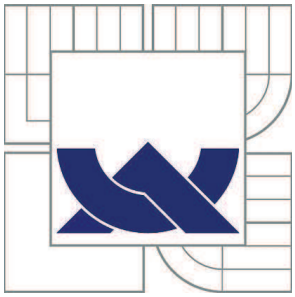
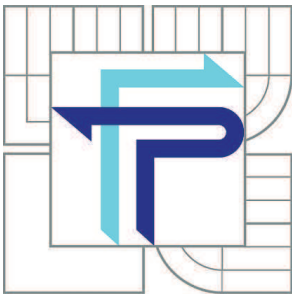


VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

BRNO UNIVERSITY OF TECHNOLOGY



FAKULTA PODNIKATELSKÁ
ÚSTAV INFORMATIKY

FACULTY OF BUSINESS AND MANAGEMENT
INSTITUTE OF INFORMATICS

MANAGEMENT INFORMAČNÍ BEZPEČNOSTI VE ZDRAVOTNICKÉM ZAŘÍZENÍ

INFORMATION SECURITY MANAGEMENT IN HEALTHCARE ORGANIZATION

DIPLOMOVÁ PRÁCE
MASTER'S THESIS

AUTOR PRÁCE — Bc. JIŘÍ HAJNÝ
AUTHOR

VEDOUCÍ PRÁCE — Ing. VIKTOR ONDRÁK, Ph.D.
SUPERVISOR

BRNO 2014

Vysoké učení technické v Brně
Fakulta podnikatelská

Akademický rok: 2013/2014
Ústav informatiky

ZADÁNÍ DIPLOMOVÉ PRÁCE

Hajný Jiří, Bc.

Informační management (6209T015)

Ředitel ústavu Vám v souladu se zákonem č.111/1998 o vysokých školách, Studijním a zkušebním řádem VUT v Brně a Směrnicí děkana pro realizaci bakalářských a magisterských studijních programů zadává diplomovou práci s názvem:

Management informační bezpečnosti ve zdravotnickém zařízení

v anglickém jazyce:

Information Security Management in Healthcare Organization

Pokyny pro vypracování:

Úvod
Cíle práce, metody a postupy zpracování
Teoretická východiska práce
Analýza současného stavu
Vlastní návrhy řešení
Závěr
Seznam použité literatury
Přílohy

Seznam odborné literatury:

ČSN ISO/IEC 27001:2006 Informační technologie - Bezpečnostní techniky - Systémy managementu bezpečnosti informací – Požadavky. Český normalizační institut, 2006.
ČSN ISO/IEC 27002:2005 Informační technologie – Bezpečnostní techniky – Soubor postupů pro řízení bezpečnosti informací. Český normalizační institut, 2005.
DOBDA L. Ochrana dat v informačních systémech. Praha: Grada Publishing, 1998. ISBN 80-716-9479-7.
DOUCEK P., L. NOVÁK a V. SVATÁ Řízení bezpečnosti informací. Praha: Professional Publishing, 2008. ISBN 80-86898-38-5.
POŽÁR J. Základy teorie informační bezpečnosti. Praha: Vydavatelství PA ČR, 2007. ISBN 978-80-7251-250-8.
POŽÁR J. Informační bezpečnost. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2005. ISBN 80-86898-38-5.

Vedoucí diplomové práce: Ing. Viktor Ondrák, Ph.D.

Termín odevzdání diplomové práce je stanoven časovým plánem akademického roku 2013/2014.

L.S.

doc. RNDr. Bedřich Půža, CSc. Ředitel ústavu	doc. Ing. et Ing. Stanislav Škapa, Ph.D. Děkan fakulty

V Brně, dne 21.04.2014

Abstrakt
Diplomová práce se zaměřuje na nasazování systému řízení bezpečnosti informací (ISMS) do zdravotnických organizací. Specifikuje, co všechno je potřeba zahrnout do tohoto procesu a na co při něm nezapomenout. Obsahuje analýzu rizik pobočky jedné vybrané společnosti, a pro ni je sepsána bezpečnostní příručka. Bezpečnostní příručka obsahuje rady a doporučení týkající se bezpečnosti z hlediska lidských zdrojů, fyzické bezpečnosti, bezpečnosti ICT a dalších aspektů, které je nutno zahrnout při nasazování ISMS do většiny zdravotnických organizací. Podle této příručky by se měla vybraná společnost řídit. V práci jsou zmíněny i zajímavé části nově vznikajícího zákona o kybernetické bezpečnosti. Předpokládá se, že zákon bude řešit také kybernetickou bezpečnost ve zdravotnictví.

Abstract
The diploma thesis focuses on implementation and deployment of information security management system (ISMS) into healthcare organizations. Specifies what is required to include in this process and what not to forget. It includes a risk analysis of a branch of the selected company, and for it is written a safety guide. Safety guide provides advice and recommendations regarding security in terms of human resources, physical security, ICT security and other aspects that should be included in the ISMS deployment in healthcare organizations. The work also reflects the newly emerging law on cyber security. It is expected that the law will also address cyber security in healthcare.

Klíčová slova
systém řízení bezpečnosti informací, ISMS, zdravotnická bezpečnost, analýza rizik, bezpečnost lidských zdrojů, fyzická bezpečnost, bezpečnost ICT, bezpečnostní směrnice, zákon o kybernetické bezpečnosti

Key words
information security management system, ISMS, health security, risk analysis, personal security, physical security, ICT security, safety guidelines, law on cyber security

Citace

HAJNÝ, J. Management informační bezpečnosti ve zdravotnickém zařízení. Brno: Vysoké učení technické v Brně, Fakulta podnikatelská, 2014. 128 s. Vedoucí diplomové práce Ing. Viktor Ondrák, Ph.D.

Čestné prohlášení

Prohlašuji, že předložená diplomová práce je původní a zpracoval jsem ji samostatně. Dále prohlašuji, že citace použitých pramenů je úplná, že jsem v práci neporušil autorská práva (ve smyslu Zákona č. 121/2000 Sb., o právu autorském a o právech souvisejících s právem autorským).

V Brně dne 30. 5. 2014

……
podpis studenta

Poděkování

Rád bych touto cestou poděkoval vedoucímu diplomové práce panu Ing. Viktoru Ondrákovi, Ph.D. a všem, se kterými jsem konzultoval za vstřícný přístup, cenné rady a připomínky, které mi pomohly při psaní této práce.

Obsah

Úvod

Motto:
Bezpečnost je tak účinná, jak je silný její nejslabší článek.

V současné době, kdy se všechny vyspělé národy světa vydávají na cestu ke znalostní společnosti, se neustále větší a větší pozornost obrací k informačním systémům a informačním a komunikačním technologiím (IS/ICT) jako významnému zdroji konkurenční výhody. Tato konkurenční výhoda spočívá ve dvou rovinách. První je jejich ovládání a schopnost jejich užívání, která dává uživatelům výhodu před těmi, kteří jich buď neumí využívat vůbec, nebo je umějí využívat pouze v omezeném rozsahu. Druhou výhodou je pak využívání obsahu informačních systémů – zejména dat, informací a znalostí, které jsou v nich uloženy a které jsou k dispozici pouze tomu, kdo ví, jak s nimi pracovat.

S výhodami přichází ale také nebezpečí ve formě zneužití, krádeže a zničení těchto majetků a zdrojů firem. Zde vystupuje do popředí zájmu právě informační bezpečnost, která v sobě zahrnuje i bezpečnost IS/ICT. Obzvlášť citlivé je pak téma bezpečnosti ve zdravotnické organizaci. Dle mého názoru není vývoj znalostí a zabezpečení IS/ICT všude stejný. Právě ve zdravotnictví se obecně mírně zanedbává. V dnešní době by lékař ve vedoucí pozici měl mít mimo svůj primární obor také velké schopnosti v administrativě, hospodaření, vyjednávání a v neposlední řadě také ve zvládání ICT technologií. Na to však většinou není ani čas ani prostor. V praxi pak většina vysoce odborných lékařů nestačí sledovat aktuální turbulentní rozvoj v této oblasti a vzniká zde řada nejen bezpečnostních hrozeb z důvodu neznalosti lékařů. Z toho důvodu jsem se rozhodl vypracovat diplomovou práci na toto téma a informovat o problematice, která zatím není v patřičném rozsahu rozvíjena.

Celá práce je rozdělena do kapitol podle zadání práce. V první kapitole je vymezen rozsah a stanoveny cíle práce. Dále je zde také popsán soubor metod a postupů zpracování.

Druhá kapitola obsahuje potřebná teoretická východiska, ze kterých je čerpáno v praktické části diplomové práce. Jsou zde vyjmenovány některé důvody, proč se zabývat informační bezpečností. Dále jsou zde vysvětleny nejdůležitější pojmy informační bezpečnosti a nastíněn systém řízení bezpečnosti informací pomocí PDCA cyklu. Kapitolu uzavírá popis metodik na správnou a dostatečně účinnou analýzu rizik a nakonec jsou uvedeny cíle informační bezpečnosti ve zdravotnictví, včetně právního prostředí, platných bezpečnostních norem a tématiky ochrany osobních údajů ve zdravotnictví.

Praktickou část mé diplomové práce otevírá kapitola 3 – Analýza současného stavu, kde je komplexně analyzována situace v mnou vybrané pobočce zdravotnické organizace z několika pohledů. Konec kapitoly představuje souhrnná analýza rizik s popisem hrozeb a zranitelností jednotlivých kategorií aktiv.

Kapitola 4 – Vlastní návrhy řešení je stěžejní obsah praktické části diplomové práce. V této kapitole jsou navrženy konkrétní opatření na pobočce mnou vybrané organizace. Jedná se o bezpečnostní příručku, která obsahuje opatření z oblasti bezpečnosti lidských zdrojů, fyzické bezpečnosti, bezpečnosti informačních a komunikačních technologií a dalších bezpečnostních aspektů. Je zde nastíněna bezpečnostní politika vzhledem k připravované legislativě.

V Závěru je zhodnocení celé práce a je zde také představeno směřování informační bezpečnosti organizace do budoucna.

1 Cíle práce, metody a postupy zpracování

1.1 Vymezení problému a cíl práce

Cílem této diplomové práce je:

I. zmapovat a popsat problematiku nasazování systému řízení bezpečnosti informací (ISMS) ve zdravotnických organizacích podle normy ČSN ISO/IEC 27799:2010

II. vytvořit bezpečnostní příručku pro možné nasazení ISMS v praxi na základě bezpečnostní analýzy konkrétní pobočky vybrané zdravotnické organizace.

Hlavními důvody k sepsání této diplomové práce jsou:

a) Čím dál častější útoky hackerů na zdravotnické organizace,
b) Nejnovější právní ochrana pro kybernetickou bezpečnost kritické infrastruktury ČR, do níž nejspíše bude patřit i většina zdravotnických organizací.

Ad a) – Příkladem zde budiž nedávný hackerský útok na nemocnici na Bulovce ze dne 12. 9. 2013, kdy došlo k následujícímu, cituji:

„Podle všech indicií došlo dnes v noci ve 3 hodiny k útoku zvenčí na počítačovou síť Nemocnice Na Bulovce. Pracovník informatiky mající noční službu rozpoznal nestandardní chování systému a zjistil přihlášení zvenčí. Situaci vyhodnotil jako rizikovou a proto okamžitě odpojil systém od vnějšího prostředí a navíc odpojil jednotlivá pracoviště mezi s sebou, aby nedošlo k úniku či mazání dat.“

Zdroj:[1]

Další indicie v tomto směru je varování ze dne 30. 04. 2014 zveřejněné na serveru instituce CSIRT provozovaného firmou CZ.NIC [2], cituji:

*„**FBI varuje před možným nárůstem kyberútoků proti poskytovatelům zdravotní péče***

Kyberútoky proti poskytovatelům zdravotní péče budou pravděpodobně narůstat. Upozorňuje na to FBI a experti dodávají, že to není žádné překvapení, protože postoj tohoto odvětví k bezpečnosti je přibližně dekádu za postojem sektoru poskytujícího finanční služby.“

V této aktualitě autoři odkazují na citlivost a zastaralost bezpečnostních systémů ve zdravotnictví, před kterými varuje FBI, zdroj:[3].

Ad b) – Práce se zaobírá také nutným minimem pro realizování důsledků nejnovějších legislativních změn, které by se měly uvést v platnost následující rok, konkrétně 1. 1. 2015, a to skrze nově připravovaný zákon o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti) a příslušných prováděcích vyhlášek. Tento zákon se bude dotýkat nejen společností a osob podnikajících v oblasti zdravotnictví, ale i ostatních subjektů, kteří jsou jakkoli spojeni s kritickou informační infrastrukturou České republiky a také kteří provozují významný informační systém (více viz dále).

1.2 Metody a postupy zpracování

Metody a postupy zpracování se budou striktně opírat převážně o platnou normativní podporu, a to normy z řady ČSN ISO/IEC 27000, jenž jsou věnovány právě systému řízení bezpečnosti informací a souvisejících metodik (např. analýza rizik apod.). Oblasti zdravotnictví je pak věnována norma ČSN ISO/IEC 27799, která bude popsána dále.

Pro praktickou část diplomové práce byla vybrána přední firma podnikající v oblasti dodavatelství specializovaných lůžkových zdravotnických služeb, která však nejen kvůli citlivosti dané problematiky (bezpečnost pacientských dat) nechce být konkrétně jmenována, a proto všechny informace o společnosti irelevantní k tématu diplomové práce (název společnosti, sídlo apod.) budou znepřesněny anebo pseudonymizovány.
Konkrétně budou všechny opatření proti rizikům a celá případová studie zaměřeny na jednu z dvaceti firemních poboček v nevelikém okresním městě. Tato pobočka je součástí areálu tamní nemocnice, která již systém řízení bezpečnosti informací podle normy ČSN ISO/IEC 27001:2006 zaveden má.

2 Teoretická východiska práce

V této kapitole si uvedeme některé vybrané teoretické podklady, z nichž se bude dále čerpat při řešení praktické části diplomové práce. Budou se týkat především teorie kolem systému řízení bezpečnosti informací a právního prostředí na území ČR. Uvedu zde několik novinek na poli bezpečnosti kritické infrastruktury ČR.

2.1 Důvody, proč se zabývat informační bezpečností

Chránit svá data je v dnešní době nevyhnutelný trend. Důvodů, proč se zabývat informační bezpečností, je tudíž hned několik.

Jako první bych uvedl pohled právní. Nejen ve zdravotnictví platí přísná pravidla a zákony o ochraně osobních a citlivých údajů (více o legislativním prostředí ve zdravotnictví – viz dále). Porušením těchto pravidel se vystavujeme nebezpečí velmi vysoké pokuty až trestu odnětí svobody za velmi vážné porušení zákona.

Dalším důvodem je bezesporu pohled morálně-etický. Tady vstupuje do věci pacient a jeho právo na soukromí a ochranu citlivých dat. Je nepředstavitelné, aby byla všechna pacientská data dostupná široké veřejnosti. Ani nemusím popisovat, jaké následky by tento stav obnášel. Každý by si mohl kupříkladu najít, že nějaký jeho známí trpí na onemocnění jater, rakovinu nebo obdobnou citlivou záležitost a to je vysoce nepřípustné.

V neposlední řadě uvedu pohled ekonomický. Pokud by v dnešní době někdo, ať už omylem, zveřejnil nebo vypustil do oběhu něčí citlivá data, vystavoval by se velikému riziku žaloby ze strany dotyčného a mohl by poté být donucen platit vysokou pokutu. Tento pohled opět souvisí s právním prostředím České republiky.

2.2 Obecné pojmy informační bezpečnosti

V této podkapitole bych nastínil některé hlavní obecné pojmy informační bezpečnosti pro uvedení čtenáře do problému. O tomto tématu bylo napsáno již velké množství knížek, a proto jen stručně popíšu oblasti, které nějakým způsobem souvisí s vybranou problematikou.

2.2.1 Základní názvosloví

- IT (Information Technology) = Informační technologie
- ICT (Information and Communication Technology) = Informační a komunikační technologie
- IS (Information System) = Informační systém
- ISMS (Information Security Management System) = Systém řízení informační bezpečnosti

Vybrané pojmy informační bezpečnosti:

Aktivum (*Asset*) – Aktiva jsou všechny hmotné i nehmotné statky, vše, co má pro majitele informačního systému jistou hodnotu. Za nejcennější aktiva se považují peníze, majetek a především data a informace, jejichž zneužití, ztráta nebo modifikace by organizaci nebo osobě způsobily určitou škodu.

Bezpečnost (*Security*) – Pod pojmem bezpečnost chápeme vlastnost nějakého objektu nebo subjektu (IS či technologie), která určuje stupeň, míru jeho ochrany proti možným škodám a hrozbám.

Hrozba (*Threat*) – Je to skutečnost, událost, síla nebo osoby, jejichž působení (činnost) může způsobit poškození, zničení, ztrátu důvěry nebo hodnoty aktiva. Hrozba může ohrozit bezpečnost (např. přírodní katastrofa, hacker, zaměstnanec aj.).

Ocenění rizik (*Risk Assessment*) – Je to proces vyhodnocení hrozeb, které působí na IS s cílem definovat úroveň rizika, kterému je systém vystaven. Cílem je zjištění, jsou-li bezpečnostní opatření dostatečná, aby snížila pravděpodobnost vzniku škody na přijatelnou úroveň.

Riziko (*Risk*) – To je pravděpodobnost, s jakou bude daná hodnota aktiva zničena nebo poškozena působením konkrétní hrozby, která působí na slabou stránku této hodnoty. Je to tedy míra ohrožení konkrétního aktiva.

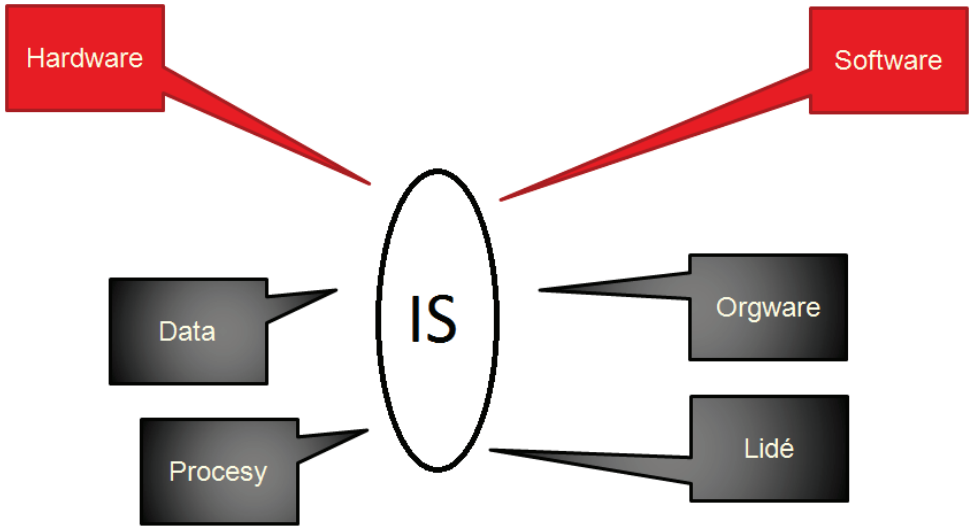
Zranitelnost (*Vulnerability*) – To je nedostatek nebo slabina bezpečnostního systému, která může být zneužita hrozbou tak, že dojde k poškození nebo zničení hodnoty aktiv. Každé aktivum je zranitelné, protože jeho hodnotu ovlivňují různé vlivy.

Převzato z [4].

2.2.2 Informační systém

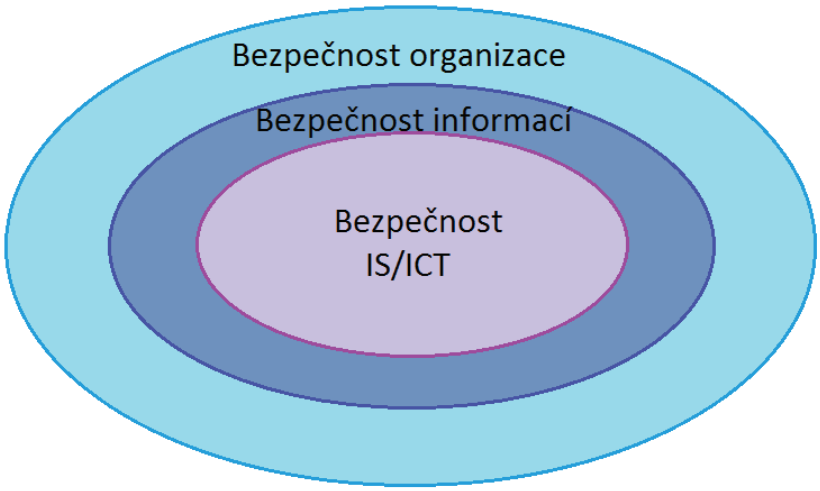
Jediná a přesná definice informačního systému neexistuje kvůli rozmanitosti terminologie. Informační systém lze však obecně chápat jako soubor vzájemně propojených informací a procesů, které s těmito informacemi pracují [5]. Skládá se z informačních a komunikačních technologií (hardware + software), dat, procesů, orgware (pravidla fungování) a lidí. Viz přiložený obrázek:

Obrázek 1 Informační systém, Zdroj: vlastní tvorba



2.2.3 Informační bezpečnost

Obrázek 2 Bezpečnost informací, Zdroj: vlastní tvorba



Bezpečnost informací (informační bezpečnost) řeší ochranu informací a dostupnost informací. Je ve vzájemném vztahu s pojmy bezpečnost organizace (která je jí nadřazená) a bezpečnost IS/ICT (podřazená bezpečnosti informací). Bezpečnost organizace má za úkol zajištění bezpečnosti objektu a tím také majetku organizace a zahrnuje v sobě i bezpečnost informací a bezpečnost IS/ICT.

Bezpečnost informací zahrnuje kromě bezpečnosti IS/ICT práci s informacemi v nedigitální podobě, což ve zdravotnictví je velmi rozšířeno (RTG snímky apod.). Bezpečnost IS/ICT chrání pouze aktiva IS podporovaná informačními a komunikačními technologiemi. Převzato z [5].

2.2.4 Požadavky na důvěryhodné a bezpečné informační systémy

Bezpečnost informačních technologií můžeme vymezit třemi základními pojmy. Jsou to:

- ***Důvěrnost*** – ochrana před prozrazením informace
- ***Integrita*** – ochrana před neoprávněnou modifikací
- ***Dostupnost*** – ochrana před neoprávněným odmítnutím služby nebo nemožností poskytnout informaci

Tyto základní požadavky na bezpečnost jsou společné pro všechny informační systémy a technologie.

Důvěrnost *(Confidentiality):* Je to utajení informací před neoprávněným přístupem. Je to charakteristika informace, která znemožňuje její odhalení neoprávněným subjektům (především lidem). Jsou to funkce, které předcházejí hrozbám neautorizovaného přístupu k informacím, a funkce, které řídí uživatelův přístup k objektům a zdrojům IS.

Integrita *(Integrity):* Je to česky řečeno celistvost, konzistence systému a dat, které informační systém obsahuje a jejich shoda s realitou. Je to taková vlastnost objektu, umožňující změnit jej pouze autorizovaným způsobem, bez jakékoliv skryté nebo úmyslné manipulace s hodnotami objektu. Integrita jako vlastnost objektu minimalizuje možnosti jeho neoprávněných změn.

Dostupnost *(Availability):* Je to vlastnost objektů, nebo celého IS, která zabraňuje neautorizovanému zadržování zdrojů. Je to tedy vlastnost IS, která zajišťuje, aby data byla na správném místě ve správný čas bez zbytečných prodlev.

Převzato z [6].

2.2.5 Komunikační bezpečnost

Komunikační cesty informačních systémů představují dnes jedno z nejdůležitějších a zároveň nejvíce zranitelných míst. Základním pojmem je počítačová síť. Počítačovou sítí budeme rozumět soustavu počítačů, serverů a jiných výpočetních systémů, které jsou propojeny navzájem pomocí spojovacích nástrojů do určité komunikační architektury. Jednotlivý uživatelé tak mohou spolu navzájem komunikovat. To však s sebou přináší jisté hrozby a mohou být jejich data napadeny za různým účelem. V literatuře se mimo názvu komunikační bezpečnost používá také pojem síťová bezpečnost či bezpečnost počítačových sítí. Jednotlivé hrozby komunikační bezpečnosti budou rozebrány v podkapitole 3.5.3 – Identifikace hrozeb a zranitelností.

Při řešení komunikační bezpečnosti se vychází z faktu, že každý samostatný počítač je již zabezpečen, považuje se za důvěryhodný a řeší se pouze ochrana komunikačních cest a informací, které přenášejí. Počítačové sítě se nejčastěji dělí na lokální a rozlehlé. Někdy lze příslušnost určité sítě do jedné z těchto kategorií určit zcela jednoznačně, zatímco jindy to může být dosti nejasné a závislé na subjektivním pohledu. Lokální počítačové sítě vznikají zpravidla z potřeby sdílet technické a

programové prostředky. Naproti tomu rozlehlé sítě vznikají především z potřeby komunikovat a provádět určité činnosti na dálku (elektronická pošta, přenos souborů na dálku). S „velikostním" kritériem lokálních a rozlehlých sítí souvisí i jejich typická topologie a vztah provozovatele sítě ke komunikační infrastruktuře. Rozlehlé počítačové sítě, které pokrývají relativně velké území, využívají přenosové cesty procházející přes veřejné prostory. Veřejné přenosové cesty zpravidla zřizuje a provozuje organizace k tomu oprávněná, takže ten, kdo takovouto síť buduje, si potřebné cesty zpravidla pronajímá od někoho jiného. Proto se pak výsledná topologie určuje i takovými faktory, jako je dostupnost a cena (za pronájem) přenosové cesty. Naproti tomu u lokálních sítí si jejich zřizovatel realizuje potřebnou infrastrukturu sám a sám je i jejím vlastníkem. Významnou odlišností je i způsob fungování přenosových mechanismů sítí. Základním prostředkem výměny dat je komunikační protokol. Pro každou vrstvu je definován alespoň jeden protokol, s jehož pomocí si entity jedné síťové vrstvy mohou předávat data. Protokolem rozumíme tedy řadu pravidel, která výměnu informace mezi příslušnými entitami realizují. Některé přenosové protokoly síťové vrstvy dokáží pracovat jak v lokálních, tak i v rozlehlých sítích (např. protokol IP rodiny protokolů TCP/IP).

V dnešní době se navíc stále více stírá rozdíl mezi lokálními a rozlehlými počítačovými sítěmi. Síťové operační systémy, určené dříve pouze pro lokální počítačové sítě, mají dnes charakteristické rysy rozlehlých sítí.

Lokální počítačové sítě

Lokální počítačové sítě (LAN, Local Area Network) mají z hlediska bezpečnosti svá specifika. Jsou to především tyto:

- Aktivní i pasivní prvky lokální sítě jsou umístěny v omezeném prostoru jedné nebo několika budov. Na její komponenty je tedy možné uplatnit různé metody fyzické ochrany.
- Lokální počítačová síť bývá zpravidla vybudována pomocí jednotné technologie a má známou topologii, podle níž lze modifikovat použité ochranné mechanismy.
- Správa lokální sítě je řízena jednoznačně definovaným síťovým administrátorem, který je podřízen vedení informačního úseku firmy,

a který může efektivně vynucovat dodržování stanovené bezpečnostní politiky ve všech komunikačních uzlech.

- Uživatelé lokální sítě jsou zpravidla zaměstnanci jedné organizace, kteří často pracují ve společném oboru a mají k sobě tedy patřičnou důvěru.

Rozlehlé počítačové sítě

Rozlehlé počítačové sítě (WAN, Wide Area Network) se od lokálních odlišují v několika aspektech, které je při řešení bezpečnostních mechanismů nutno zvážit.

- Rozlehlé datové komunikační sítě se často provozují jako veřejné sítě, které se vůči uživateli sice jeví z hlediska použitého protokolu jako systém transparentní, avšak u nichž je současně implementována vysoká inteligence zpracování dat, plně řízená a kontrolovaná poskytovatelem a provozovatelem sítě, a to nezávisle na jejích uživatelích. I při sebelepším technickém zabezpečení sítě vždy hrozí riziko zneužití pozice provozovatele sítě a technických prostředků, kterými disponuje.
- Technické prostředky přenosu dat fyzicky sdílejí uživatelé různých informačních systémů, a tedy i různých organizací.
- Alespoň část komunikačních tras prochází veřejnými prostory a je tedy veřejně přístupná.

Referenční model ISO/OSI

Organizace ISO se v roce 1977 rozhodla vytvořit standard pro provoz komunikačních systémů. Úkolem přípravy nového standardu pověřila svou subkomisi SC 16. Výsledkem práce komise bylo vymezení sedmivrstvového modelu a specifikace úkolů, které by tyto vrstvy měly zajišťovat. Úplný název celého standardu je „Reference Model of Open Systems Interconnection" (Referenční model propojování otevřených systémů), a označení normy je ISO 7498 (v praxi je obvykle označován zkratkou ISO/OSI).

Referenční model ISO/OSI je díky své otevřené architektuře zatím dostatečně pružný vůči rostoucím technologickým požadavkům. Na každý systém účastnící se komunikace je nahlíženo tak, jako by byl sestaven z hierarchicky závislých subsystémů, které jsou uspořádány do vrstev. Platí zásada, že komunikace se odehrává pouze mezi entitami ze stejné vrstvy. Komunikace tedy probíhá virtuálně pouze v horizontálním směru. Mezi vrstvami existuji ve vertikálním směru rozhraní, kterých vždy využívá

vyšší vrstva, aby fyzicky zajistila své komunikace ve směru horizontálním. Vždy nižší vrstva zajišťuje transparentní informační kanál mezi vrstvami, které jsou od ní nejblíže vyšší.

Základní metody ochrany komunikací

Fyzické zabezpečení komunikačních zařízení

Jeho cílem je dosáhnout takového stavu, kdy jsou všechny komunikační cesty sítě zabezpečeny tak, aby na nich nebylo možné provádět odposlech, nebylo možné je přerušit nebo nějak zjistit obsah přenášených dat. Tohoto stavu lze ovšem dosáhnout pouze v malých lokálních sítích a za nemalých finančních nákladů. V době nastupující celosvětové komunikace, kdy všechny dálkové spoje považujeme za nebezpečné, je tento úkol asi opravdu neřešitelný a bezpečnost komunikace se realizuje jinak. Lokální sítě lze fyzicky zabezpečit několika způsoby. Jsou to:

Ochrana komunikačních portů (Port protection) – zablokování možnosti použití prázdných síťových zásuvek síťového rozvodu. Je to doplňková ochrana mechanismu autentizace uživatele koncové stanice. Aktivní prvek sítě má ve své databázi uložena čísla komunikačních portů – zásuvek a k nim připojených síťových karet, konkrétně jejich MAC adres. Při komunikaci s tímto portem se porovnává i jeho MAC adresa, která musí souhlasit s údajem v databázi. V opačném případě je přístup k síti odepřen.

Řízení připojení do sítě. Musí se zabránit tomu, aby si nemohl kdokoliv připojit cokoliv do sítě bez vědomí správce sítě. Základní princip je neumísťovat přípojky k počítačové síti do nechráněných — veřejně přístupných prostorů.

Zabezpečení kabelových spojů. Musí se zabránit tomu, aby se na tyto spoje mohl někdo neoprávněně napojit. Požadavek se realizuje ochranou především strukturovaných kabelů (ukládají se např. do zdi, do trubek naplněných inertním plynem, kdy podtlakové čidlo kontroluje vnitřní atmosférický přetlak a při narušení potrubí vydá signál k ukončení komunikace), nebo vizuální kontrolou (nejutajovanější část informačního systému ministerstva obrany jedné nejmenované světové velmoci má kabelové spoje uloženy na kabelových lávkách ve výšce pasu tak, aby se daly neustále opticky kontrolovat, a členové ozbrojené hlídky musejí být navíc z různých oblastí země, aby se předem neznali).

Zamezení elektromagnetického vyzařování kabelů vhodným stíněním.

Řízení směru toku dat

Je to jedna ze základních metod ochrany rozsáhlých komunikačních sítí. Je založena na tom, že nastavíme komunikační trasy pro chráněná data tak, že definujeme cesty, po kterých mohou procházet a kterým důvěřujeme, a zakážeme cesty, kam informace jít nesmějí. Tato technologie řízení tras se realizuje aktivními síťovými prvky – směrovači (routers), mosty (bridges) a popř. rozbočovači (hubs). Tyto filtry při předávání paketů z jedné podsítě do druhé povolují průchod pouze podle předem definovaných pravidel. Filtruje se na základě adresy odesílatele, adresy příjemce a typu paketu. Pokud se tyto filtrační členy použijí jako spojovací a zabezpečovací článek mezi interní – privátní sítí organizace a vnější veřejnou sítí, označují se jako firewall. Ty nekontrolují komunikaci uvnitř interní sítě, ale kontrolují a řídí tok informací s vnějším prostředím. Tato ochrana však nikterak nebrání odposlechu a modifikaci dat během jejich přenosu.

Dvoubodové spoje

Jsou z pohledu bezpečnosti nejvýhodnější. Např. u terminálových sítí se ke každému terminálu přenášejí pouze data pro něj určená, a dojde-li k odposlechu, nelze zjistit nic o informacích posílaných na ostatní terminály. Tyto výhody však samozřejmě neplatí pro dvoubodový spoj mezi dvěma sítěmi.

Vícebodové spoje

Tuto architekturu má většina současných sítí. Informace vysílané z jednoho uzlu sítě mohou zachytit i všechny ostatní uzly sítě. Pro odposlech je to ideální prostředí. Základní metodou ochrany komunikací je vhodný návrh topologie sítě a její rozdělení na co nejvíce samostatných úseků oddělených inteligentními spojovacími členy. Tyto úseky je však nutno navrhovat nejen podle jejich umístění, ale především podle toho, jaké informace zpracovávají.

Kryptografická ochrana

Základním bezpečnostním mechanismem na komunikačních sítích je šifrování, které zabezpečuje tři služby: důvěryhodnost, integritu a autentizaci. Kryptografickou ochranu dat lze aplikovat na všechny oblasti komunikací. Je ideálním řešením všude

tam, kde nelze zabezpečit spojovací kanál a chránit datový tok. I přes tyto zřejmé výhody se však zatím kryptografie v běžných aplikacích výrazněji nerozšířila. Výhledově, s nástupem globální komunikace, je ale možné očekávat masové nasazení kryptografických metod ochrany informací, především technologie hardwarových šifrovačů a automatické distribuce veřejných šifrovacích klíčů. Provozovatel informačního systému musí také počítat s tím, že se zavedením šifrování souvisí také nutnost distribuce a správy šifrovacích klíčů a certifikačních autorit pro jejich ověřování.

Převzato z [7].

2.3 Systém managementu informační bezpečnosti (ISMS)

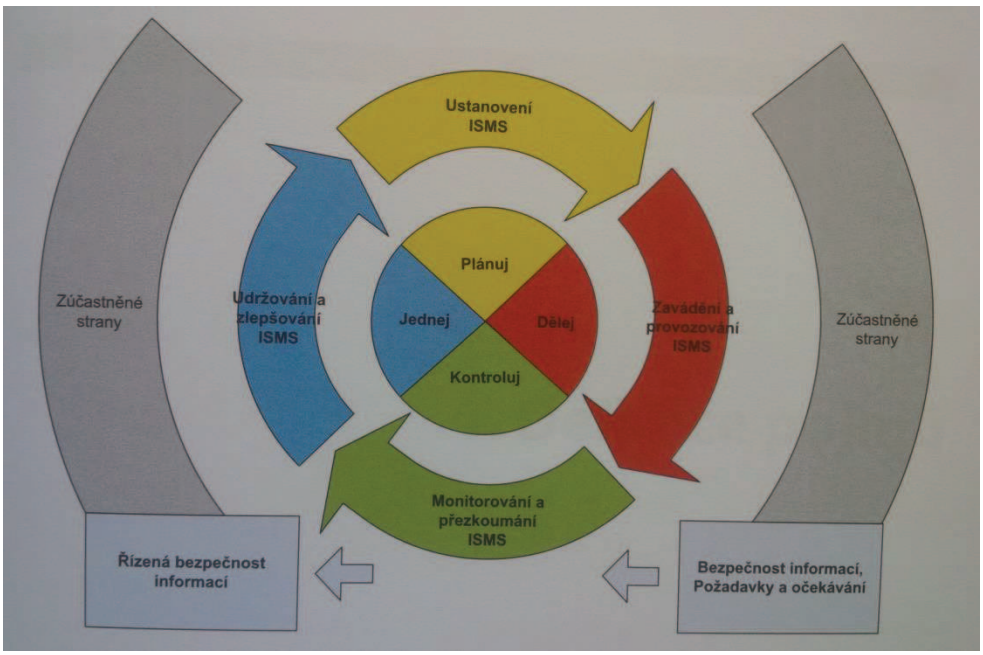
Systém řízení informační bezpečnosti je část celkového systému řízení organizace, založená na přístupu organizace k rizikům činností, která je zaměřena na ustanovení, zavádění, provoz, monitorování, přezkoumání, údržbu a zlepšování bezpečnosti informací. Systém řízení v sobě zahrnuje organizační strukturu, politiky, plánovací činnosti, odpovědnosti, mechanismy, postupy, procesy a zdroje. Obdobně jako ostatní systémy řízení je založen na modelu PDCA. Byly zde definovány následující čtyři etapy životního cyklu systému řízení:

- **Ustanovení ISMS** – cílem této etapy je upřesnit rozsah a hranice, kterých se řízení bezpečnosti týká, stanovit jasné manažerské zadání a na základě ohodnocení rizik vybrat nezbytná bezpečnostní opatření.
- **Zavádění a provoz ISMS** – cílem této etapy je účelně a systematicky prosadit vybraná bezpečnostní opatření do chodu organizace.
- **Monitorování a přezkoumání ISMS** – hlavním cílem této etapy je zajištění zpětné vazby a pravidelného sledování a hodnocení úspěšných i nedostatečných stránek řízení bezpečnosti informací.
- **Údržba a zlepšování ISMS** – cílem poslední etapy je realizace možností zlepšování systému řízení bezpečnosti informací ať už soustavným zlepšováním systému nebo odstraňováním zjištěných slabin a nedostatků.

Převzato z [7]

2.3.1 PDCA cyklus

Obrázek 3 Model PDCA v ISMS, Zdroj: [5]



Na obrázku 3 lze vidět koncept modelu PDCA a jeho jednotlivé fáze. Koncept PDCA poprvé použil ve svých pracích W. E. Deming a formuloval v něm zásady vymezení určitého systému řízení, přes jeho realizaci až po cyklickou snahu o jeho permanentní zlepšování. Koncept PDCA byl původně použit pro inovaci a nasazování systému řízení v průmyslu. V současné době se stal tento přístup základem pro mezinárodní standardy v oblasti integrovaného systému řízení, včetně oblasti řízení bezpečnosti informací. Převzato z [7]. Jde o metodu postupného zlepšování např. kvality výrobků, služeb, procesů, aplikací či dat probíhající formou opakovaného provádění čtyř základních činností:

- PLAN (plánuj) – naplánování zamýšleného zlepšení (záměr)
- DO (dělej) – realizace plánu
- CHECK (kontroluj) – ověření výsledků realizace oproti původnímu záměru
- ACT (jednej) – úpravy záměru i vlastního provedení na základě ověření a plošná implementace zlepšení do praxe.

Součástí modelu PDCA je také dokumentace každé jeho etapy jako jedna z klíčových částí celého modelu.

Převzato z [5].

2.3.2 Fáze PLAN

Podkapitoly 2.3.2 – 2.3.5 jsou převzaty z [7].

Tato etapa se v systému řízení bezpečnosti informací nazývá Ustanovení ISMS. **Má zásadní dopady na fungování ISMS během jeho celého životního cyklu.** Při ní jsou upřesněny správné formy řešení bezpečnosti informací. Kromě definice rozsahu ISMS a odsouhlasení **Prohlášení o politice ISMS** (závazek vedení podniku podporovat informační bezpečnost) patří mezi kritické činnosti provedení analýzy rizik a výběr vhodných bezpečnostních opatření pro snížení vlivu existujících rizik, čemuž se budeme věnovat v následujících kapitolách. Tato etapa by měla být ukončena souhlasem vedení se zavedením ISMS podle potřeb organizace, zjištěných při analýze a zvládání rizik ISMS. Více o metodikách analýzy rizik bude popsáno v kapitole 2.4 – Metodika analýzy rizik.

2.3.3 Fáze DO

Tato etapa se v systému řízení bezpečnosti informací nazývá Zavádění a provoz ISMS. Soustředí se na prosazení všech bezpečnostních opatření tak, jak byla navržena v odchozí etapě při ustanovení ISMS. Důležité je především připravit dílčí plány, kde jsou upřesněny termíny, odpovědné osoby apod. Všechna bezpečnostní opatření by měla být zdokumentována v tzv. **Příručce bezpečnosti informací** a mělo by dojít k vysvětlení bezpečnostních principů všem uživatelům a manažerům.

Během této etapy je nezbytné provést následující činnosti:

- Formulovat dokument Plán zvládání rizik a započít s jeho zaváděním.
- Zavést plánovaná bezpečnostní opatření a zformulovat Příručku bezpečnosti informací, která upřesní pravidla a postupy aplikovaných opatření v definovaných oblastech bezpečnosti informací podle normy ČSN ISO/IEC 27002.
- Definovat program budování bezpečnostního povědomí a provést přípravu a zaškolení všech uživatelů, manažerů a odborných pracovníků nejen z úseku informatiky.
- Upřesnit způsoby měření účinnosti bezpečnostních opatření a sledovat stanovené ukazatele.

- Zavést postupy a další opatření pro rychlou detekci a reakci na bezpečnostní incidenty.

Samozřejmostí je pak řízení zdrojů, dokumentů a záznamů ISMS. Nestačí pouze postupovat dle dohodnutých pravidel, ale je nutné i shromažďovat podklady pro další fázi monitorování. Pro umožnění kontroly správnosti fungování ISMS je podstatné vytvořit definovaná pravidla pro tvorbu, schvalování, distribuci a aktualizaci dokumentace řízení bezpečnosti (včetně odebírání, zneplatnění a skartace již neplatných verzí dokumentů). Současně je podstatné vytvářet záznamy o jednotlivých provedených úkonech ISMS, kde se objeví základní informace o provedené činnosti (identifikace osoby, která činnost prováděla, termín a místo realizace, výsledky provedené činnosti atd.). Způsob vytváření takovýchto záznamů musí být v souladu relativně snadného dohledání určitých přesně definovaných skupin aktivit (vyhledání určitých typů činností, realizovaných v určitém období či určitou osobou nebo zařízením). Převzato z [7].

2.3.3.1 Plán zvládání rizik

Je to důležitý dokument, který popisuje všechny činnosti ISMS, které jsou potřebné pro řízení bezpečnostních rizik, stanovené cíle a priority těchto činností ISMS, omezující faktory a potřebné zdroje (personální, finanční, technologické, znalostní apod.). Jeho významným prvkem je též jednoznačné určení osobní zodpovědnosti za provádění jednotlivých naplánovaných činností.

Východiskem pro sestavení jsou především dva základní zdroje informací. V počátečních fázích se jedná o podklady, které jsou získány při ustanovení ISMS (výsledky řízení rizik ze zprávy o hodnocení rizik a z prohlášení o aplikovatelnosti). Tyto dva dokumenty určují bezpečnostní potřeby a míru jejich realizace.

Druhým významným zdrojem údajů jsou podněty získané při pravidelném přehodnocování ISMS vedením organizace, které by měly být shromážděny ve zprávě o stavu ISMS. Tyto dovolují do plánu promítnout zkušenosti s fungováním ISMS. Převzato z [7].

2.3.3.2 Příručka bezpečnosti informací

Při prosazování vybraných bezpečnostních opatření je potřeba definovat stanovená pravidla a odpovědnosti s tím související. To se nejčastěji děje za pomoci dokumentů jako jsou bezpečnostní politiky a bezpečnostní směrnice apod., které určují dlouhodobě platné bezpečnostní principy, pravidla, zásady a odpovědnosti a které jsou často souhrnně nazývány jako příručka bezpečnosti informací.

Je zde potřeba rozlišovat různé úrovně připravovaných dokumentů. Na té nejvyšší úrovni jsou to především dokumenty, které si vyžaduje systém řízení a které jsou s ohledem na požadavky ISMS povinné (např. rozsah ISMS, politika ISMS, zpráva o hodnocení rizik, prohlášení o aplikovatelnosti, plán zvládání rizik apod.). Tyto dokumenty mají svoje specifické místo v systému a tomu je často podřízena i jejich forma.

Ve druhé úrovni je dokumentace, která slouží k podpoře prosazování ISMS a vždy by měla být přizpůsobena konkrétnímu ISMS. Důležitým prvkem při tvorbě této dokumentace je definice dílčích procesů a postupů, které zajišťují efektivní prosazení dílčích bezpečnostních opatření. Proto je důležité definovat kdo, co kdy, kde a jak má učinit.

Na nejnižší úrovni bezpečnostní dokumentace se nacházejí tzv. pracovní postupy. Tyto dokumenty by měly podrobně vysvětlovat úkony, které jsou nezbytné pro naplnění dílčích procesů. Ne vždy je tato úroveň nezbytná a často může být řešena odkazem na příslušnou dokumentaci použitých technických systémů.

Je potřeba pamatovat na to, že hlavním cílem tvorby je předání určených informací nějaké cílové skupině (ať už manažerům, uživatelům, správcům apod.). Tomu by se měl podřídit i způsob popisu a vyjadřování. Mírou kvality dokumentů není počet popsaných stránek, ale srozumitelnost a schopnost cílové skupiny se podle stanovených předpisů chovat. K tomu mohou přispět i jiné formy sdílení informací, než klasické sepisování příruček. Převzato z [7].

2.3.3.3 Prohlubování bezpečnostního povědomí

Za tímto pojmem se skrývá promítnutí všech definovaných pravidel a postupů do skutečného chování všech odpovědných pracovníků a uživatelů. Tento jednoduchý cíl je nicméně velmi složitým úkolem, který vyžaduje vysoké a systematické úsilí. Je to trvalý a nekonečný proces, který často rozhoduje o skutečné efektivitě ISMS. Převzato z [7].

2.3.3.4 Měření účinnosti ISMS

Dalším důležitým tématem, které je spojováno s prosazováním efektivního řízení bezpečnosti, je měření účinnosti aplikovaných bezpečnostních opatření. Tady je potřeba definovat a pravidelně sledovat objektivní údaje o skutečném fungování systému řízení bezpečnosti, na základě kterých je vhodné provádět všechna důležitá rozhodnutí.

Proces řízení účinnosti systému řízení bezpečnosti informací v organizaci není nikterak jednoduchý a je nutné jej mít na zřeteli již v okamžiku návrhu celého ISMS, protože velmi podstatné kroky pro měření efektivnosti a její vyhodnocování jsou již součástí první etapy životního cyklu. O opravdové účelnosti a účinnosti ISMS se rozhoduje již v etapě plánování.

Tehdy probíhá vstupní analýza rizik a z její kvality bezprostředně vychází i kvalita navrženého ISMS. Významný vztah k účinnosti celého navrhovaného ISMS má také přístup vrcholového vedení organizace a jeho kompetence. V této etapě je také nutné zohlednit i další zákonné případně jiné úpravy, kterými se organizace musí řídit a které vycházejí z její celkové strategie.

Jaké následky má případná chyba ve specifikaci ISMS a jaká je výše relativních nákladů spojených s jejím odstraněním, je uvedeno v následující tabulce:

Tabulka 1 Relativní náklady na odstranění chyby v ISMS [7]

Etapa PDCA modelu	Výše relativních nákladů v %
Plánuj	1,0
Dělej	6,5
Kontroluj	15,0
Jednej	100,0

Fáze DO se věnuje z pohledu vedení relativně nejjednodušší činnosti – realizaci projektů. Zde padá hlavní odpovědnosti za úspěch systému řízení účinnosti zejména na bedra projektových manažerů. Hlavním problémem v této fázi je zajistit integraci systému monitorování dat pro vyhodnocování efektivnosti do celkového

monitorovacího systému organizace. Ve fázi CHECK jsou hlavními činnostmi týmu připravujícího řízení účinnosti ISMS následující:

- definice počátečních hodnot ukazatelů měření účinnosti ISMS,
- testování systému měření,
- vlastní sběr dat a monitorování ISMS v provozu,
- sběr podkladů pro průběžný audit ISMS.

Ukazatele pro měření bezpečnosti informací lze podle předmětu měření rozdělit do následujících základních skupin:

- finanční,
- personální,
- technické - ukazatele provozu IS/ICT.

Měření účinnosti systému řízení bezpečnosti informací není v současné praxi řízení informatiky organizací absolutní prioritou. Lze předpokládat, že ve velmi krátké době, zejména díky nasazování metodik pro řízení informatiky jako jsou COBIT a ITIL, dojde na obvyklé otázky vedení společností i v oblasti bezpečnosti informací.

Převažují ukazatele technické – de facto provozní – které byly navrženy pro reálný provoz IS/ICT v organizacích a byly v něm i ověřeny. Významným rizikem nasazení všech finančních ukazatelů je skutečnost, že je velmi obtížné odlišit finance, které jsou použity na bezpečnost informací nebo které byly použity na vlastní provoz. Proto i vypovídací schopnost finančních ukazatelů je velmi omezená a jejich důvěryhodnost závisí především na odpovědnosti pracovníků, kteří je vykazují. Obdobný problém je i při vyčíslování ztrát způsobených bezpečnostními incidenty. Velmi často jsou vykazovány pouze přímé ztráty např. zničená data a náklady na jejich opětovné pořízení, málokdy ovšem jsou do nákladů bezpečnostního incidentu zahrnuty i náklady na práci bezpečnostních techniků a ostatních pracovníků, kteří za svoji práci dostanou mzdu, ale nikdo ji ani doprovodné náklady již nerozúčtuje k odpovídajícímu bezpečnostnímu incidentu.

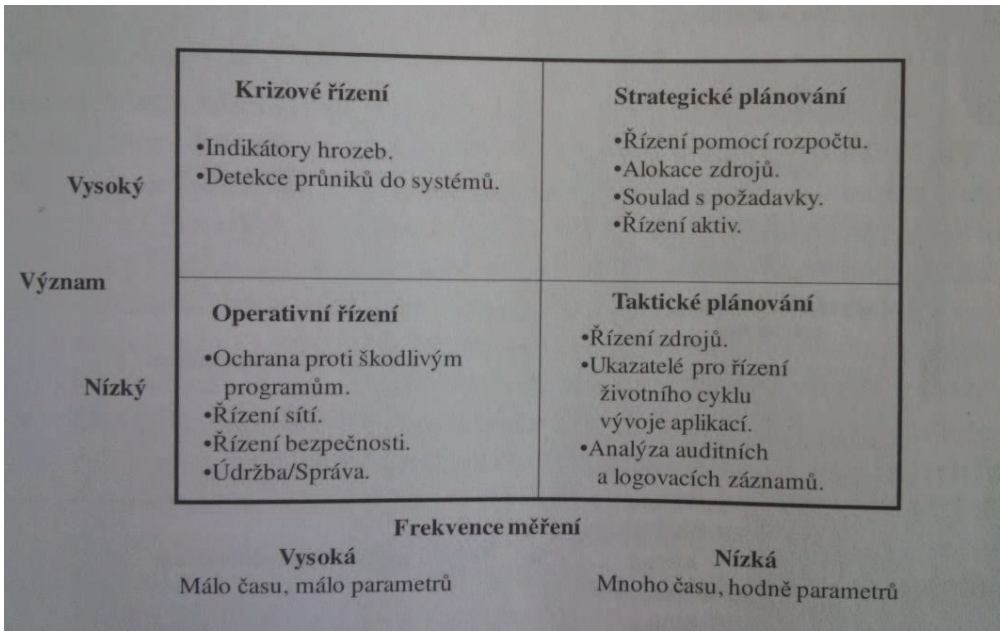
Daleko důležitější, než znát nazpaměť celé seznamy ukazatelů, je mít celkovou vizi, jak jich využívat v různých a měnících se podmínkách organizací. Každý ukazatel potřebuje pro svůj výpočet určitý čas, kromě datových zdrojů, popisu metadat pro svůj výpočet, je také definován frekvencí svého výpočtu.

Různé situace v organizacích vyžadují nasazení rozličných ukazatelů a také různou frekvenci jejich výpočtů. Zvláště pro ty procesy, které jsou uvedeny v kvadrantu „Krizové řízení", je lepší provádět v kratších časových úsecích.

Ukazatele s velmi krátkou dobou zjišťování pomáhají vedení organizací sledovat efektivnosti v denních nebo týdenních odstupech, což je mnohem operativnější než výkazy a zprávy, které vedení dostává jednou za rok. To má za následek, že ukazatele, které má vedení dostávat často a v krátkých časových úsecích, musí být navrženy tak, aby nebyly příliš náročně na čas sběru dat a na svůj výpočet.

Schéma a strategický koncept ukazatelů pro měření bezpečnosti informací spolu s jejich významem a doporučenou frekvencí jejich zjišťování je uveden na následujícím obrázku. Převzato z [7].

Obrázek 4 Schéma ukazatelů, Zdroj: [7]



Řízení účinnosti ISMS patří k nedílným součástem jeho životního cyklu. Celková skladba a doporučení pro nasazení jednotlivých ukazatelů jsou ovšem závislé na podmínkách nasazení ISMS v určité organizaci. Proto jsou vděčným tématem výzkumů a pozorování pro odborníky v oblasti informatiky. Jiný přístup k měření účinnosti ISMS mívají pracovníci, kteří jsou v organizaci zodpovědní za finance, finanční řízení nebo efektivitu investic. Pro ně není smyslem a cílem vyvinout koherentní systém pouze pro měření účinnosti bezpečnosti informací nebo IS/ICT. Jejich cílem je vybudovat systém pro měření efektivnosti organizace jako celku, resp. efektivnosti jejích hlavních

procesů. Systém pro sledování celkové efektivnosti organizace pak vychází z měření efektivnosti hlavních procesů, následně procesů vedlejších a podpůrných.

Volba správných ukazatelů je v praxi klíčovým faktorem, který má zásadní vliv na prohlubování účinnosti řízení bezpečnosti. Zde platí dvě klíčové rady. První je skryta v přísloví „Méně někdy bývá více". Zejména z počátku nasazení ISMS je důležité připravit méně ukazatelů, které se ovšem především soustředí na prioritní oblasti řízení. Větší rozsah ukazatelů pak následně připravit až po získání základních zkušeností z chování systémů řízení.

Druhou radou je omezení snahy o získávání absolutních ukazatelů. Pro kvalitní rozhodování je postačující relativní představa. A lze jen připomenout, že každé zvyšování přesnosti je spojeno s významně vyššími náklady. Převzato z [7].

2.3.4 Fáze CHECK

Tato etapa se v systému řízení bezpečnosti informací nazývá Monitorování a přezkoumání ISMS. Hlavním úkolem této etapy je zajistit účinné zpětné vazby. V souvislosti s tímto požadavkem by mělo dojít k prověření všech aplikovaných bezpečnostních opatření a jejich důsledků na ISMS. Vlastní ověření začíná u přímé kontroly odpovědných osob ze strany jejich nadřízených nebo bezpečnostním manažerem. Důležitou roli sehrává také nezávislé posouzení fungování a účinnosti ISMS pomocí interních auditů. Obecným cílem je připravit dostatek podkladů o skutečném fungování ISMS, které budou předloženy vedení za účelem přezkoumání, zda je realizace ISMS v souladu s obecnými potřebami organizace.

Během této části je nezbytné provést následující činnosti:

- Monitorovat a ověřit účinnost prosazení bezpečnostních opatření.
- Provést interní audity ISMS, jejichž náplň pokryje celý rozsah ISMS.
- Připravit zprávu o stavu ISMS a na jejím základě přehodnotit ISMS na úrovni vedení organizace (včetně revize zbytkových a akceptovaných rizik).

Základní zpětnou vazbou je provádění kontrol ze strany všech osob, které mají za fungování ISMS nějakou odpovědnost a to na všech manažerských úrovních. Tyto osoby by měly dohlížet na to, zda bezpečnostní opatření patřící do jejich kompetence naplňují očekávání, která byla do nich při zavádění vkládána. Součástí kontrol musí být

i schopnost včasné detekce chyb, úspěšných i neúspěšných pokusů o narušení bezpečnosti či schopnost sledování bezpečnostních událostí a včasné detekce bezpečnostních incidentů.

Druhým prvkem zpětné vazby je provádění interních auditů ISMS, které na rozdíl od kontrol zajišťují potřebný nezávislý pohled na fungování ISMS. Audity by měly prověřovat oba aspekty ISMS. Prvním je dodržování procesních pravidel, kde je dominantním kritériem auditu naplňování požadavků ČSN ISO/IEC 27001. Druhým aspektem je prověřování fungování jednotlivých bezpečnostních opatření, která jsou pro potřeby ISMS zavedena. Zde se jako kritérium uplatňuje norma ČSN ISO/IEC 27002.

Třetí prvkem je pak přezkoumání ISMS vedením organizace. Mělo by probíhat pravidelně a to nejméně jednou za rok, u nově zavedených ISMS i častěji. Mezi vstupy patří všechna podstatné informace o fungování ISMS za hodnocené období. Na základě těchto podnětů dochází k posouzení silných a slabých stránek ISMS (SWOT analýza). Mezi důležité výstupy SWOT analýzy patří:

- Zlepšení účinnosti ISMS (zvyšování míry bezpečnosti při snižování náročnosti realizace bezpečnostních opatření).
- Aktualizace ohodnocení rizik a souvisejících plánů pro zvládání rizik.
- Nezbytné úpravy procesů, pravidel a postupů ISMS.
- Plánovaná náročnost ISMS na zdroje (finanční, lidské, technologické apod.) v dalším období.

Převzato z [7].

2.3.5 Fáze ACT

Tato etapa se v systému řízení bezpečnosti informací nazývá Údržba a zlepšování ISMS. Jedná se především o to, že v této fázi by mělo docházet ke sběru podnětů ke zlepšení ISMS a k nápravě všech nedostatků, tzv. neshod, které se v ISMS objevují.

Během této části zavádění je nezbytné provést následující činnosti:

- zavádět identifikované možnosti zlepšení ISMS (především na základě přehodnocení vedením),
- provádět odpovídající opatření k nápravě a preventivní opatření pro odstranění nedostatků.

Převzato z [7].

2.3.5.1 Soustavné zlepšování ISMS

Je velmi důležité do každého systému řízení zapracovat účinnou zpětnou vazbu. Ta by měla fungovat tak, že na jedné straně získává podněty, které mohou vést k efektivnějšímu fungování ISMS, na druhé straně musí tato vazba odhalovat nedostatky a jejich příčiny a vhodným způsobem na tyto podněty reagovat. Podstatným prvkem zlepšování je především využití pozitivní zpětné vazby. Je žádoucí, aby se zlepšování ISMS opíralo o zkušenosti aktivních účastníků. Ti by měli osoby odpovědné za ISMS informovat o svých podnětech, které mohou fungování ISMS zlepšit. Nápady pocházející z reálné praxe jsou vždy nenahraditelné a jejich důslednému zapracování by měla být věnována velká pozornost. Osoby odpovědné za ISMS by si podnětů pocházejících od řadových pracovníků měly vážit. To ale neznamená vždy jen jejich bezhlavé zavedení. U všech podnětů je nutné zvážit jejich přímé i nepřímé dopady a důsledky pro organizaci a s tím související rizika. Dobré promyšlení dopadů někdy může znamenat zamítnutí či úpravu požadavku, což by mělo být vhodným způsobem projednáno s původním navrhovatelem. Pro rozvoj ISMS je důležité i prohlubovat motivaci pracovníků na účasti při všech činnostech spojených s ISMS v tom, aby sdíleli své zkušenosti a aby otevřeně navrhovali, co je vhodné a žádoucí na chodu ISMS zlepšit. Převzato z [7].

2.3.5.2 Odstraňování nedostatků ISMS

Pro odstraňování nedostatků existují dvě formy opatření:

- opatření k nápravě a
- preventivní opatření.

Opatření k nápravě je reaktivní formou řešení nedostatku. V tomto případě se již nedostatek nějakým způsobem projevil (často označujeme tuto skutečnost neshodou) a je potřeba na něj vhodným způsobem reagovat.

Naproti tomu **preventivní opatření** je proaktivní formou řešení nedostatků ISMS. V tomto případě se vychází z toho, že se zjištěný nedostatek ještě neprojevil, ale další odklad jeho řešení by mohl vést k tomu, že se v budoucnu nějaká negativní událost objeví a způsobí vážnější problémy. Důležitým a nenahraditelným prvkem odstraňování nedostatků oběma způsoby je objasnění příčin, které k těmto nedostatkům vedly. V tomto smyslu nestačí pouze zjednat nápravu u konkrétní neshody. Je důležité se

podívat na souvislosti a opatření realizovat tak, aby se omezily možnosti opakování tohoto nedostatku. Před prosazením obou typů opatření je též nezbytné posoudit, zda zvolené opatření dostatečně zamezí opakování nedostatku a případně pokryje jeho příčiny.

Postupy pro řešení opatření k nápravě a preventivních opatření musí být zdokumentovány a všechny činnosti s nimi spojené musí být zaznamenány a zahrnuty do dokumentace. Po zavedení opatření je též důležité přezkoumat, zda zvolená opatření skutečně zajistila očekávanou změnu účinnosti ISMS. Praktické zkušenosti ukazují, že často podceňovanou příčinou nedostatků je nedostatečná znalost požadavků, které ISMS vyžaduje. Běžným projevem této příčiny jsou nejasnosti či neznalosti souvislostí a vazeb mezi dílčími požadavky. ISMS se stává souborem dílčích úkonů, nikoli však systémem řízení. Převzato z [7].

2.4 Metodika analýzy rizik

Analýza rizik je prováděna za účelem identifikace zranitelných míst informačního systému organizace (BS ISO 17799:2005).

Následně zachycuje seznam hrozeb působících na IS a stanovuje rizika příslušná každému zranitelnému místu a hrozbě. Účelem takového dokumentu je snížení rizik na přijatelnou úroveň, respektive akceptaci zbytkových rizik tam, kde je jejich minimalizace neefektivní. Značení a míry jsou následující.

P - Pravděpodobnost vzniku a existence rizika:

1 - Nahodilá.

2 - Nepravděpodobná.

3 - Pravděpodobná.

4 - Velmi pravděpodobná.

5 - Trvalá.

R - Míra rizika

0-10: Bezvýznamné riziko.

11-20: Akceptovatelné riziko.

21-30: Mírné riziko.

31-60: Nežádoucí riziko.

61-125: Nepřijatelné riziko.

Popis dělení rizik:

Bezvýznamné riziko (zanedbatelné): není vyžadováno žádné zvláštní opatření. Nejedná se však 0 100% bezpečnost, proto je nutno na existující riziko upozornit a uvést např. organizační a výchovná opatření — RIZIKO MOŽNO PŘIJMOUT.

Akceptovatelné riziko (přijatelné): riziko přijatelné se souhlasem vedení. Je nutno zvážit náklady na případné řešení nebo zlepšení; v případě, že se nepodaří provést technická bezpečnostní opatření ke snížení rizika, je třeba zavést alespoň vhodná a přiměřená opatření organizační dle místních podmínek. Většinou postačuje školení apod. - MOŽNÉ RIZIKO, ZVÝŠIT POZORNOST.

Mírné riziko (významné): i když urgentnost opatření není tak závažná jako u rizik nežádoucích, je zpravidla nutno bezpečnostní opatření realizovat dle zpracovaného plánu podle rozhodnutí vedení firmy. Prostředky na snížení rizika musí být implementovány ve stanoveném časovém období — POTŘEBA NÁPRAVNÉ ČINNOSTI.

Nežádoucí riziko: vyžadující urychlené provedení odpovídajících bezpečnostních opatření snižujících riziko na přijatelnější úroveň, na snížení rizika se musí přidělit potřebné zdroje. Je-li toto riziko spojeno se značnými následky, musí se provést jeho další vyhodnocení tak, aby se přesněji stanovila pravděpodobnost vzniku úrazu, jako podklad stanovení potřeby dosažení snížení rizika - VYSOKÉ RIZIKO, BEZPROSTŘEDNÍ BEZPEČNOSTNÍ OPATŘENÍ.

Nepřijatelné riziko: nepřípustné, značné, kritické riziko, permanentní možnost úrazů, závažné nehody, nutnost okamžitého zastavení činnosti, odstavení z provozu do doby realizace nezbytných opatření a nového vyhodnocení rizik a přijetí potřebných opatření. Práce nesmí být zahájena nebo v ní nesmí být pokračováno, dokud se riziko nesníží! - VELMI VYSOKÉ RIZIKO, ZASTAVIT ČINNOST!

Analýza rizik se rozděluje:

- Analýza rizik – hrubá úroveň.
- Analýza rizik – neformální přístup.
- Analýza rizik – kombinovaný přístup.
- Analýza rizik – podrobný přístup.

Nejčastější průběh analýzy rizik je popsán ve směrnici ČSN ISO/IEC TR 13335-3. Doporučuje se použít kombinaci metod pragmatické (neformální) a detailní analýzy

rizik. Nejprve je provedena počáteční analýza rizik na hrubé úrovni pro všechny systémy IT. U systémů, které budou identifikovány jako významné pro činnost organizace, případně vystavené vysokým rizikům, provádíme podrobnou analýzu rizik.

Analýza rizik na hrubé úrovni bere v úvahu hodnotu systému IT pro činnost organizace a zpracovávaných informací a rizika z pohledu činnosti organizace. Pro rozhodnutí, který přístup je pro který systém IT vhodný, bude mít význam zohlednění následujících skutečností:

- jakých cílů má být použitím systému IT dosaženo;
- úroveň investic do tohoto systému IT (vývoj, údržba, nahrazení);
- aktiva systému IT, kterým organizace přiřazuje určitou hodnotu;
- stupeň činnosti organizace závisící na systému IT (zda funkce, které organizace považuje pro své přežití za kritické nebo efektivní, jsou závislé na tomto systému IT).

Po tomto základním rozdělení budeme vědět, které systémy jsou vhodné k nasazení základního přístupu (ty méně kritické, nákladné apod.) a ty u kterých je nutné provést podrobnou analýzu rizik.

Pragmatická analýza rizik je **neformální přístup**, který není založen na strukturovaných metodách, ale využívá znalosti a zkušenosti jednotlivců. Výhodou této volby je, že nevyžaduje obvykle mnoho zdrojů nebo času. K provedení této neformální analýzy není nutné se naučit nové dodatečné dovednosti a tato analýza je provedena rychleji než podrobná analýza rizik. Existuji také nevýhody. Například bez detailních seznamů kontrol vzrůstá pravděpodobnost opomenutí některých důležitých detailů a je obtížné obhájit implementaci ochranných opatření ve vztahu k rizikům odhadnutým tímto způsobem. V minulosti byly některé přístupy založeny na zranitelnostech, tedy byla implementována bezpečnostní ochranná opatření založená na identifikovaných zranitelnostech, aniž by se zvažovalo, zda existovaly konkrétní hrozby, které by pravděpodobně využily tyto zranitelnosti neboli zda vůbec existovala reálná potřeba ochranných opatření. Tímto způsobem může docházet ke zbytečnému navyšování finančních prostředků.

Kombinovaný přístup je třetí možností. Nejprve se provede počáteční analýza rizik na hrubé úrovni pro všechny systémy IT, která se soustřeďuje u každého případu na hodnotu systému IT pro činnost organizace a na vážná rizika, jimž je systém IT

vystaven. U systémů IT, které jsou identifikovány jako významné pro činnost organizace a/nebo vystavené vysokým rizikům, by měla být přednostně provedena podrobná analýza rizik. Pro všechny zbývající systémy IT by měl být zvolen základní přístup. Tato volba, která je kombinací nejlepších charakteristik možností umožňuje minimalizaci času a úsilí věnovaného na identifikaci ochranných opatření, přičemž stále ještě zajišťuje, že jsou vysoká rizika systému chráněna příslušným způsobem.

Podrobný přístup je podrobná (detailní) analýza rizik systému IT obsahující identifikaci souvisejících rizik, a odhad jejich velikosti.

Podrobná analýza rizik zahrnuje hloubkovou revizi v každém z těchto kroků:

Stanovení hranic revize

Stanovení hranic revize bude provedeno ještě před identifikací a hodnocením aktiv. Pečlivá definice hranic nám umožní vyvarovat se zbytečných činností. Jinými slovy budeme definovat, kterých prvků se bude analýza rizik týkat, například aktiva IT.

Identifikace aktiv

Aktivum je komponenta nebo část celkového systému, které organizace přímo přiděluje hodnotu, a pro kterou tudíž organizace požaduje ochranu. Při identifikaci aktiv vezmeme v úvahu i to, že systém IT netvoří jen HW a SW.

Ohodnocení aktiv

Ve chvíli, kdy budeme mít identifikovaná aktiva, musíme k nim přiřadit hodnoty. Tyto hodnoty reprezentují význam aktiv pro činnost organizace. Vstupní údaje pro hodnocení aktiv budou zajištěny vlastníky a uživateli aktiv, například formou dotazníku, případně pomocí interview. Hodnota aktiv nemusí být určena finančním ohodnocením, ale například z hlediska nepříznivých dopadů na činnost organizace, plynoucí ze ztráty důvěrnosti, integrity, dostupnosti, individuální odpovědnosti, autenticity a spolehlivosti. Pro výpočet ohodnocení aktiva je možno využít různé postupy. Nejjednodušším a také nejpoužívanějším je tzv. součtový algoritmus.

Principem je podíl součtu: (Důvěrnost + Dostupnost + Integrita) / 3

Hodnocení hrozeb

Hrozba představuje možnost poškodit zkoumaný systém IT a jeho aktiva. Hrozby mohou být přírodního nebo lidského původu a mohou být úmyslné nebo náhodné. Jako základní katalog hrozeb lze využít seznam uvedený v normě ČSN ISO/IEC TR 13335-3 v příloze C. Hodnocení hrozeb bude dáno do souvislosti s identifikovanými aktivy společnosti.

Odhad zranitelnosti

Tento odhad odhalí slabá místa ve fyzickém prostředí, organizaci, postupech, personálu managementu, administraci HW, SW, nebo komunikačním zařízení, která mohou být využita zdrojem hrozby a způsobit tak škodu na aktivech.

Identifikace plánovaných a existujících ochranných opatření

Součástí analýzy rizik je tzv. identifikace plánovaných nebo existujících bezpečnostních opatření. Výsledkem tohoto kroku je mimo výše zmiňovaného, také seznam všech existujících a všech plánovaných bezpečnostních opatření.

Výběr ochranných opatření

Princip ochranných opatření spočívá v minimalizaci případných rizik. Aby se usnadnil popis různých typů ochranných opatření, jsou v rámci normy zavedeny kategorie ochranných opatření. Podrobně jsou popsána v normě ČSN ISO/ IEC TR 13335-4. Mezi nejdůležitější jsou řazena tzv. „všeobecně aplikovatelná ochranná opatření". Jedná se o základní kategorie:

- řízení a politiky bezpečnosti IT,
- kontrola bezpečnostní shody,
- řešení incidentů,
- personální opatření,
- provozní problémy,
- plánování kontinuity činnosti organizace,
- fyzická bezpečnost.

Odhad rizik

Cílem tohoto kroku je identifikovat a odhadnout rizika, kterými jsou aktiva vystavena. Tedy jednoduše řečeno, musíme zjistit, co nám hrozí a proč nám ta rizika hrozí.

Přijetí rizik

Po identifikaci a odhadu rizik, po výběru a revizi ochranných opatření však vždy zůstávají tzv. zbytková rizika. Úplně bezpečný systém je pouze teoretická hypotéza, ke které se lze v reálném provozu pouze limitně blížit. Zbytková rizika mohou být rozdělena a být buď akceptována (akceptace rizika) nebo neakceptována. Jestliže riziko není akceptováno, probíhá znovu výběr ochranných opatření a odhadování rizik. Je zde vysoké riziko, že může být přijato dodatečně ochranné opatření, které je příliš nákladné nebo z hlediska bezpečnosti zbytečné.

Politika bezpečnosti systému IT

Politika bezpečnosti systému IT by měla obsahovat podrobnosti požadovaných ochranných opatření a popis, proč jsou nezbytná.

Plán bezpečnosti IT

Jedná se o shrnující dokument, který stručně popisuje veškeré akce, které se musí uskutečnit, aby mohla být implementována ochranná opatření.

Převzato z [5].

2.5 Cíle bezpečnosti informací ve zdravotnictví

Hlavními cíli jsou:

- zachování **důvěrnosti** dat,
- zachování **dostupnosti** a
- zachování **integrity** informační bezpečnosti.

V oblasti zdravotnictví je soukromí pacientských dat závislé na zachování důvěrnosti osobních zdravotních údajů pacientů. Mezi opatření, které by mělo být přijato v rámci integrity dat, má nejvyšší prioritu **mlčenlivost**. Je nutné stanovit kontrolu integrity dat a další systémová zabezpečení. Pokud by byla integrita dat špatně nastavená, mohlo by to pacienta v nejhorším případě ohrozit na životě. Stejně tak by jej mohla ohrozit špatná dostupnost dat. Z tohoto důvodu je nezbytné nastavit vysokou úroveň dostupnosti dat. Jako každý systém je i zdravotní informační systém vystavován možným síťovým útokům zvenčí, ale také z řad běžných uživatelů (v tomto případě lékařů) uvnitř organizace. Proto je důležité věnovat zvýšenou pozornost nastavení zabezpečení a eliminovat tak útoky v systému. Bezpečný IS lze definovat jako systém, který chrání informace během jejich vstupu, zpracování, uložení, přenosu a výstupu proti ztrátě dostupnosti, integrity a důvěrnosti a po jejich likvidaci proti ztrátě důvěrnosti. Bezpečnost IS je velmi rozsáhlý problém, který tvoří řetěz složený z článků - jednotlivých podoblastí bezpečnosti. *Bezpečnost je tak účinná, jak je silný její nejslabší článek.*

Informačními technologiemi je zpracováváno stále více a více informací s velkou hodnotou. Pokud hovoříme v souvislosti s informačními technologiemi o *zpracovávání informací*, pak tím rozumíme použití těchto technologií k uchovávání, přenosu, vyhodnocování a prezentaci informací. Poněvadž se mnohdy jedná o informace s nezanedbatelnou hodnotou (např. zdravotní záznamy, elektronické platební nástroje, výsledky vývoje nebo výzkumu, obchodní záměry), musí být chráněny tak:

- aby k nim měly přístup pouze oprávněné osoby
- aby se zpracovávaly nefalšované informace
- aby se dalo zjistit, kdo je vytvořil, změnil, nebo odstranil
- aby nebyly jakýmkoliv způsobem vyzrazeny
- aby byly dostupné tehdy, když jsou potřeba

Jakákoliv opatření směřující ke zvýšení úrovně bezpečnosti IS skutečně pouze odčerpávají dostupné finanční prostředky a nejsou zdrojem žádného výnosu ani zisku. Naopak, zabezpečení ve větší či menší míře klade překážky do cesty procesům, které kladný finanční tok zajišťují. Zpomalují práci chráněného systému, zvyšují nároky na uživatele, kteří jsou nuceni zvládat manipulaci s bezpečnostními mechanismy, a vyžadují zásahy do organizace pracovních postupů, bez nichž by implementace bezpečnosti byla zbytečná. Přesto investice do bezpečnosti IS jsou účelným vynaložením prostředků, protože chrání klíčové procesy před poškozením a informace před zcizením a následným zneužitím. Nepodílejí se na tvorbě zisku, ale zajišťují jeho udržení. Redukují riziko a minimalizují ztráty v případě, že riziková událost nastane.

Od zdravotnických pracovníků nemůžeme očekávat, že si přivlastní praktické znalosti toho, jak se mají zabezpečit informační systémy, neboť toto je technická a vysoce komplexní záležitost. Je však nezbytné, aby zdravotničtí pracovníci chápali, proč je důležité udržovat bezpečné prostředí pro zdravotní záznamy, které shromažďují o pacientech a rozuměli, jak lze tohoto cíle dosáhnout.

Zdravotní záznamy obsahují jak informace související s fyzickým či duševním zdravím pacientů, tak informace vztahující se k poskytování zdravotnické péče ze strany zdravotníků nebo zdravotnických zařízení. Způsob poskytování zdravotní péče se uchovává v odborných záznamech, které obsahují pozorování a názory lékařů a dalšího zdravotnického personálu. Tato data neukládají do zdravotního záznamu pouze zdravotníci, kteří se přímo starají o pacienta (lékaři, zdravotní sestry), ale také další pracovníci ve zdravotnictví (patologové, rentgenologové, farmaceuti), nezdravotnický personál, který pomáhá zdravotníkům (sekretářky a administrativní pracovníci) a dokonce i pacienti sami. Tato rozmanitost zdrojů a způsobů využití dat v osobním zdravotním záznamu s sebou přináší problémy se zabezpečením jak v tradičních záznamech vedených v papírové formě, tak i v elektronických zdravotních záznamech.
Vzrůstající zájem o použití elektronického zdravotního záznamu, který by mohl případně nahradit tradiční záznam na papíru, přináší do popředí zájem o bezpečnost informací. Tím se nemyslí pouze důvěryhodnost neboli správný stupeň utajení osobních údajů, ale také jejich integrita, což znamená jejich přesnost a úplnost, a jejich dostupnost, kdy a kde je jich zapotřebí. Vytvoření odpovídajícího právního prostředí musí předcházet zavedení elektronického zdravotního záznamu do zdravotnické praxe.

Elektronické zdravotní záznamy se uchovávají, zpracovávají nebo přenášejí prostřednictvím ICT. Umožňují, aby informace v nich obsažené využívalo současně více osob, a jsou základním kamenem pro rozvoj telemedicínských aplikací. Toho lze však dosáhnout pouze pomocí vhodné počítačové infrastruktury. Je možné, aby ti, kteří umí prozkoumat a pozměnit počítačové záznamy, tak učinili bez nejmenší stopy po své činnosti. Počítačové záznamy lze označit značkou uživatelů, kteří je vytvářejí nebo upravují, ale postupy, jakými je dnes často potvrzována identita uživatele (např. kontrola pomocí hesla) má ještě mnoho slabin. Do informačních systémů lze však zavést nástroje, které budou kontrolovat respektování zákona o ochraně osobních dat 101/2000 Sb., a zabezpečí údaje před různými způsoby zneužití. Avšak tato omezení při používání dat musí být v balanci s nutností zpřístupnit informace těm, kteří mají potřebu a nárok je znát.

Prevence neoprávněných úprav je v hardwarovém zabezpečení nesmazatelnosti záznamu. Dále neoprávněným úpravám brání kódování záznamu nebo jeho *digitální podpis* (popisuje zákon 260/2001 Sb.). Jeho přijatelnost nebyla dosud jako dostatečný důkaz ve většině evropských zemí na soudech ještě testována. Další otázkou je *archivace* elektronických zdravotních záznamů. Existuje minimální období požadované v evropských zemích, po které musí být data archivována. V některých případech je to třicet a více let. Tradiční záznamy (papírové záznamy nebo rentgenové snímky) v tak dlouhých časových obdobích obvykle vydrží. Situace s elektronickými médii je již méně uspokojivá. Záznamy na magnetických médiích, jako jsou např. pásky nebo disky se časem ničí a musí být pravidelně obnovovány. Optická média, jako je DVD-ROM, jsou sice stabilnější, přesto však nemají definovanou *úložnou životnost*. Navíc nelze zaručit, že vybavení a software ke čtení takovýchto digitalizovaných informací bude dostupný i po třiceti letech při současné rychlosti, s jakou se vyvíjí technologie. Zvláště problematická je tato otázka v případě pohotovostních multimediálních zdravotnických záznamů, kde se používají složité komprimační algoritmy, aby se omezily paměťové nároky na uchovávání snímků s vysokým rozlišením, video a audio záznamy. Konverze takových záznamů z jednoho formátu do druhého může zapříčinit ztrátu informací nebo zhoršení kvality snímků. Nelze tudíž zaručit, že digitální lékařské snímky uložené v dnešních archivech budou dostupné ve stejné kvalitě i po třiceti letech. Záznamy, které se označují digitálním podpisem, budou

nerozluštitelné, ztratí-li se klíč. Bezpečnější kódovací schémata, která se doporučují pro použití ve zdravotnictví, se spoléhají na důvěryhodnou třetí stranu, která má klíče k údajům. Protože je důležitá dlouhodobá dostupnost klíčů, navrhuje se, aby klíče k údajům zůstávaly v rámci veřejné organizace.

Zdravotnické informační systémy musí být pod přísnou kontrolou, aby se zajistila kvalita a minimálně by se mělo očekávat, že tyto systémy budou vyhovovat normě *ČSN ISO 9001:2000*. Je nutné, aby zdravotnictví rychle zavedlo takové normy, které zajistí bezpečné prostředí pro citlivé zdravotní údaje.

Zatímco technická řešení mohou předcházet zneužívání informačních systémů s elektronickými osobními zdravotními záznamy, zůstávají uživatelé pro zabezpečení největší hrozbou. Hlavně proto, že se o systémy nestarají a používají nevyhovující postupy.

2.5.1 Právní prostředí ve zdravotnictví

V této podkapitole bude popsán současný stav zákonů a vládních institucí zabývajících se kybernetickou bezpečností. Kvůli nedávným nebezpečným DDoS útokům se začalo rozšiřovat povědomí o nutnosti chránit svá data a přístup k nim v rozsahu kritické infrastruktury. Bylo ustaveno několik institucí, aby bylo toto důležité téma řešeno centrálně na úrovni státu. Mezi tyto nové instituce patří například Národní centrum kybernetické bezpečnosti (NCKB), Rada pro kybernetickou bezpečnost (RKB), Vládní CERT a jiné soukromé instituce jako například CSIRT provozovaný firmou CZ.NIC, které spolupracují při ochraně bezpečnostních záležitostí. Dále zde již nějakou dobu působí Národní bezpečnostní úřad (NBÚ).

2.5.1.1 Národní bezpečnostní úřad

Od samého začátku působení NBÚ (jak podle zákona č. 148/1998 Sb., tak i podle nového zákona č. 412/2005 Sb.) je postavení NBÚ stále stejné - je orgánem výkonné moci, je ústředním správním úřadem pro oblast ochrany utajovaných informací a bezpečnostní způsobilosti. To znamená, že je zařazen jednak mezi ústřední úřady a jednak mezi správní úřady.

Tyto dvě skutečnosti (postavení) se plně odrážejí ve stanovených pravomocích (kompetencích), oprávněních a úkolech. NBÚ není v žádném případě zpravodajskou

službou, ani není pověřen žádnými vyšetřovacími pravomocemi ve smyslu oprávnění orgánů činných v trestním řízení.

NBÚ vydáním osvědčení (fyzické osobě i podnikateli) nebo dokladu o bezpečnostní způsobilosti (fyzické osobě) garantuje, že u jeho držitele nebyly zjištěny žádné skutečnosti, které by mu bránily mít přístup k utajovaným informacím nebo vykonávat citlivé činnosti. Tím přispívá velkou měrou k ochraně informací důležitých pro obranné, vojenské, bezpečností, ekonomické a mezinárodně politické záměry a cíle České republiky, a tím i k ochraně zdraví, života a majetku občanů. Stát tak může svěřit své strategické informace při zajišťování obrany státu, při boji proti terorismu, při odhalování závažné trestné činnosti, při zajišťování důležitých ekonomických zájmů i zájmů, k jejichž ochraně se zavázal v rámci mezinárodní spolupráce, i výkon citlivé činnosti subjektům, které skýtají záruku, že tyto informace ani citlivou činnost nezneužijí nejen ve svůj prospěch, ale i ve prospěch např. cizích „špionážních“ služeb apod.

Současný proces mezinárodního sbližování vyžaduje mezinárodní spolupráci bezpečnostních orgánů a složek i ostatních subjektů podílejících se na zajišťování bezpečnosti České republiky. Tuto mezinárodní spolupráci zejména s orgány NATO a EU rozvíjí a prohlubuje i NBÚ. Výměna informací na mezinárodní úrovni i v oblasti ochrany utajovaných informací je velmi důležitá a přispívá k ujednocování postupů, forem spolupráce a k možnosti uznávání jednotlivých bezpečnostních oprávnění vydaných národními bezpečnostními úřady. [10]

2.5.1.2 Rada pro kybernetickou bezpečnost

Rada pro kybernetickou bezpečnost byla ustavena usnesením vlády č. 781 ze dne 19. října 2011. Rada je poradním orgánem předsedy vlády pro oblast kybernetické bezpečnosti. Cílem její činnosti je zároveň podpora výkonu gesční a koordinační role Národního bezpečnostního úřadu v oblasti kybernetické bezpečnosti vyžadující součinnost státních institucí a subjektů kritické infrastruktury.

Hlavními úkoly Rady jsou:

- koordinace činnosti státních institucí v oblasti kybernetické bezpečnosti a přispívání k zajištění plnění závazků meziresortní povahy,
- koordinace státních institucí při plnění závazků v oblasti kybernetické bezpečnosti, které vyplývají z členství České republiky v mezinárodních organizacích a koordinace zastupování České republiky v mezinárodních organizacích a v dalších zahraničních aktivitách souvisejících s kybernetickou bezpečností,
- aktivní vytváření podmínek pro hladké fungování spolupráce mezi členy Rady,
- řešení aktuálních otázek kybernetické bezpečnosti a předkládání odborných návrhů a doporučení vládě,
- sledování plnění závěrů z jednání Rady jejími členy,
- shromažďování, analýza a vyhodnocení údajů o stavu zajištění kybernetické bezpečnosti poskytovaných členy Rady,
- příprava návrhu zprávy o stavu zajištění kybernetické bezpečnosti České republiky, která je pravidelně předkládána předsedou vlády vládě jako výchozí dokument, který stanovuje priority a z nich vyplývající úkoly v oblasti kybernetické bezpečnosti pro nadcházející období,
- spolupráce s externími odbornými subjekty a využívání jejich výstupů v zájmu zajišťování kybernetické bezpečnosti České republiky. [9]

2.5.1.3 Národní centrum kybernetické bezpečnosti

Dne 19. října 2011 přijala vláda České republiky usnesení č. 781 o ustavení Národního bezpečnostního úřadu gestorem problematiky kybernetické bezpečnosti a zároveň národní autoritou pro tuto oblast. Přílohou usnesení je Statut Rady pro kybernetickou bezpečnost. Na základě přijatého usnesení vzniklo Národní centrum kybernetické bezpečnosti (NCKB), jako součást Národního bezpečnostního úřadu, se sídlem v Brně.
Úlohou centra je koordinace spolupráce na národní i mezinárodní úrovni při předcházení kybernetickým útokům i při návrhu a přijímání opatření při řešení incidentů i proti probíhajícím útokům.

Hlavní oblasti činnosti centra [9]:

- provozovat Vládní CERT České republiky (GovCERT.CZ)
- spolupráce s ostatními národními CERT® týmy a CSIRT týmy
- spolupráce s mezinárodními CERT® týmy a CSIRT týmy
- příprava bezpečnostních standardů pro jednotlivé kategorie organizací v ČR
- osvěta a podpora vzdělávání v oblasti kybernetické bezpečnosti
- výzkum a vývoj v oblasti kybernetické bezpečnosti

2.5.1.4 Vládní CERT

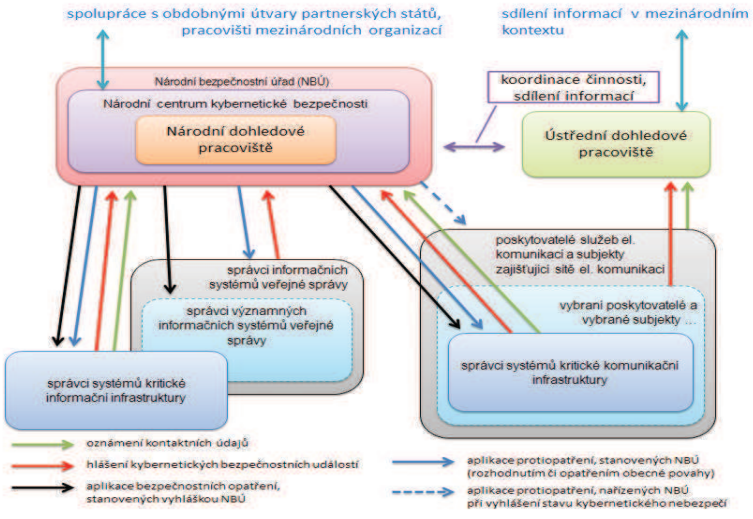
Vládní CERT (GovCERT.CZ) a týmy typu CSIRT hrají klíčovou roli při ochraně Kritické informační infrastruktury. Každá země, která má své kritické systémy připojeny do internetu, musí být schopna efektivně a účinně čelit bezpečnostním výzvám, reagovat na incidenty, koordinovat činnosti při jejich řešení a účelně působit při předcházení incidentům.

Úlohou těchto týmů je zároveň působit jako prvotní zdroj bezpečnostních informací a pomoci pro orgány státu, organizace i občany. Neméně důležitou roli hrají při zvyšování vzdělanosti v oblasti bezpečnosti na internetu. [9]

2.5.1.5 Systém komunikace podle zákona o kybernetické bezpečnosti

Pro ilustraci ještě dodávám obrázek, který popisuje strukturu a propojení komunikace mezi subjekty, kterých se týká zákon o kybernetické bezpečnosti:

Obrázek 5 Struktura komunikace podle zákona o kybernetické bezpečnosti, Zdroj:[8]



2.5.1.6 Aktuální novinky

02. 01. 2014

Vláda České republiky ve čtvrtek 2. ledna 2014 schválila Návrh zákona o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti). Tento návrh zákona připravil a předložil Národní bezpečnostní úřad. Návrh zákona bude předložen k dalšímu legislativnímu projednávání v Parlamentu České republiky.

08. 01. 2014

Národní bezpečnostní úřad upozorňuje, že dnem 1. ledna 2014 nabývá účinnosti zákon v oblasti ochrany utajovaných informací, a to zákon č. 303/2013 Sb., kterým se mění některé zákony v souvislosti s přijetím rekodifikace soukromého práva.

21. 02. 2014

Národní bezpečnostní úřad vypracoval k návrhu zákona o kybernetické bezpečnosti, který byl předložen k dalšímu legislativnímu procesu do Parlamentu České republiky, návrh prováděcího předpisu, kterým je vyhláška o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti (vyhláška o kybernetické bezpečnosti). Návrh vyhlášky o kybernetické bezpečnosti zejména naplňuje a rozvádí první pilíř zákona o kybernetické bezpečnosti - bezpečnostní opatření, neboli požadavky na standardizaci kritické informační infrastruktury a významných informačních systémů.

Případné připomínky odborné veřejnosti k návrhu vyhlášky bylo možno uplatnit do 17. března 2014.

Pro vypracování podkapitol 2.5.1.1 – 2.5.1.5 bylo čerpáno z [9], [10].

2.5.1.7 Zákony

Zde vyjmenuji několik hlavních platných zákonů, kterými se musí řídit a které musí respektovat české zdravotnické organizace:

- zákon č. 499/2004 Sb. o archivnictví a spisové službě a o změně některých zákonů v platném znění
- zákon č. 240/2000 Sb. o krizovém řízení a o změně některých zákonů (krizový zákon) v platném znění
- zákon č. 106/1999 Sb. o svobodném přístupu k informacím v platném znění
- zákon č. 412/2005 Sb. o ochraně utajovaných informací a o bezpečnostní způsobilosti v platném znění
- zákon č. 101/2000 Sb. o ochraně osobních údajů a o změně některých zákonů v platném znění

2.5.1.8 Ostatní právní předpisy (v rámci Evropské Unie)

ČR, jakožto člen EU, je povinna respektovat a následovat nařízení pocházející z Evropské Unie, zde jsou vyjmenována ta nejdůležitější nařízení:

- směrnice rady č. 1991/250/EHS o právní ochraně počítačových programů
- směrnice EU 1995/46/ES o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů
- směrnice 2002/58/ES o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací (Směrnice o soukromí a elektronických komunikacích)
- směrnice rady č. 2001/264/EC, kterou se přijímají bezpečnostní předpisy Rady
- nařízení Evropského parlamentu a Rady 2001/45/ES o ochraně fyzických osob v souvislosti se zpracováním osobních údajů orgány a institucemi Společenství a o volném pohybu těchto údajů

Zabývat se blíže veškerými platnými zákony a nařízeními je nad rámec této diplomové práce.

2.5.2 Bezpečnostní normy ve zdravotnictví

Základem bezpečnostních norem jsou zde normy z řady ČSN ISO/IEC 27000, které do detailů popisují komplexní zavedení ISMS do nějaké organizace a všechny aspekty k tomu související, jako je například řízení rizik, metriky, auditování, různé oborové charakteristiky apod. Speciální místo pak zabírá norma ČSN ISO/IEC 27799, která je určena pro řízení bezpečnosti informací ve zdravotnických organizacích.

2.5.2.1 ČSN ISO/IEC 27799

Tato mezinárodní norma poskytuje pokyny zdravotnickým a jiným organizacím, jak nejlépe zajistit důvěrnost, integritu a dostupnost osobních zdravotních informací zavedením ČSN ISO/IEC 27001 Tato norma se zaměřuje na management bezpečnosti informací v rezortu zdravotnictví a v jeho specifických provozních podmínkách. Zatímco ochrana a bezpečnost osobních informací je důležitá pro všechny jednotlivce, společnosti, instituce a vlády, v sektoru zdravotnictví musí být splněny zvláštní požadavky, aby tak byla zajištěna důvěrnost, integrita, auditovatelnost a dostupnost osobních zdravotních informací. Zdravotnické informace jsou považovány za nejdůvěrnější ze všech druhů osobních informací. Ochrana této důvěrnosti je nezbytná, pokud má být zajištěno soukromí subjektů zdravotní péče. Integrita zdravotnických informací musí být chráněna, aby tak bylo zajištěno bezpečí pacientů. Důležitou součástí této ochrany je zajištění auditovatelnosti celého životního cyklu informací. Dostupnost zdravotnických informací je také rozhodující z hlediska efektivity výkonu zdravotní péče. Systémy zdravotnické informatiky musí splňovat zvláštní požadavky, aby byly akceschopné při přírodních katastrofách, systémových selháních a při útocích typu odmítnutí služby. Ochrana důvěrnosti, integrity a dostupnosti zdravotnických informací tudíž vyžaduje odbornou způsobilost v oblasti rezortu zdravotnictví. Potřeba efektivního managementu bezpečnosti IT ve zdravotnictví naléhavě stoupá s rostoucím počtem bezdrátových a internetových technologií v poskytování zdravotní péče. Pokud nejsou správně zavedeny, zvyšují tyto technologie rizika důvěrnosti, integrity a dostupnosti zdravotnických informací. Ve všech zdravotnických organizacích jsou nezbytné přísné kontroly přímo v místě s cílem chránit jim svěřené zdravotnické informace bez ohledu na velikost, umístění a formu poskytování služeb. Existuje mnoho odborných zdravotnických pracovníků, kteří fungují samostatně nebo v malých

klinikách a kterým chybí specializované IT zdroje na řízení bezpečnosti informací. Zdravotnické organizace proto musí mít jasné, stručné a zdravotně-specifické pokyny týkající se výběru a provádění těchto kontrol. Tento návod musí být přizpůsobitelný široké škále poskytovatelů služeb ve zdravotnictví, různé velikosti, umístění či formy. Konečně v souvislosti s elektronickou výměnou osobních zdravotních údajů mezi odbornými zdravotnickými pracovníky Je zde jasný přínos v přijetí společných doporučení pro řízení bezpečnosti informací v oblasti zdravotní péče. ISO/IEC 27002 je již široce používána pro zdravotnickou informatiku managementu bezpečnosti IT prostřednictvím působení národních či regionálních směrnic v Austrálii, Kanadě, Francii, Nizozemí, Novém Zélandu, Jižní Africe a Velké Británii. Zájem roste i v jiných zemích. Tato mezinárodní norma staví na zkušenostech těchto států a jejich úsilí při řešení bezpečnosti osobních zdravotních informací a je určena jako doprovodný dokument k ČSN ISO/IEC 27002. Není určena k nahrazení ČSN ISO/IEC 27002 nebo ČSN ISO/IEC 27001. spíše se jedná o doplnění těchto obecnějších norem. Tato mezinárodní norma aplikuje ČSN ISO/IEC 27002 do oblasti zdravotní péče způsobem, který pečlivě zvažuje vhodné uplatnění bezpečnostních kontrol za účelem ochrany osobních informací. V některých případech vedly tyto úvahy jeho autory k závěru, že použití určitých kontrolních cílů ČSN ISO/IEC 27002 je nezbytné, pokud mají být osobní zdravotní informace odpovídajícím způsobem chráněny. Tato mezinárodní norma tudíž klade omezení v aplikaci některých bezpečnostních kontrol definovaných v ČSN ISO/IEC 27002. V oblasti zdravotnictví je možné, aby organizace (řekněme nemocnice), byla certifikována ČSN ISO/IEC 27001 bez předchozího schválení, nebo dokonce bez přijetí této mezinárodní normy. Je třeba doufat, že se mezi zdravotnickými organizacemi rozšíří jak snaha o zlepšení bezpečnosti osobních zdravotních informací, tak i přísnější kritéria pro poskytování zdravotní péče. Všechny cíle bezpečnostní kontroly popsané v ČSN ISO/IEC 27002 jsou důležité pro zdravotnickou informatiku, ale některé kontroly vyžadují další vysvětlení, aby mohly být použity co nejlépe k ochraně důvěrnosti, integrity a dostupnosti zdravotnických informací. Existují i další specifické požadavky. Tato mezinárodní norma poskytuje další pokyny, které jsou snadno pochopitelné a přijatelné pro osoby odpovědné za bezpečnost zdravotnických informací. Norma nezastupuje učebnici počítačového zabezpečení, ani nepřepisuje to, co už bylo uvedeno v ČSN ISO/IEC 27002 a ČSN ISO/IEC 27001. Existuje mnoho

bezpečnostních požadavků, které jsou společné pro všechny počítačové systémy, ať již jsou používány v oblasti finančních služeb, výroby, průmyslu nebo v jakémkoliv jiném organizovaném úsilí. Zde je zaměřena intenzivní pozornost na bezpečnostní požadavky, vyžadované specifickými výzvami při předávání elektronických zdravotnických informací, které podporují poskytnutí péče. Čerpáno z normy [11].

2.5.3 Ochrana osobních údajů ve zdravotnictví

Údaje zdravotnické dokumentace jsou více citlivé na ochranu v porovnání s informacemi uchovávanými v jiných oborech. Informace o nemocném se úzce dotýká každého individua a speciální zákony zabezpečují závazné postupy při ochraně soukromí nemocného. Jako příklad může sloužit *Evropská směrnice o ochraně občanů* týkající se zpracování a přenosu jejich osobních dat. Právní status elektronických záznamů je stále v řadě evropských zemí nedostatečně definován. Prvním problémem je uznávání autorských práv v případě počítačového softwaru. Protože se informace nepřechovávají ve fyzické formě, jako je např. papír nebo film, není snadné přijmout je jako důkaz u soudu. Postupně se však tato situace začíná měnit. Uvádím následující direktivy Evropského parlamentu a doporučení Rady Evropy pro tuto oblast:

- *95/46/EC:* Zpracování osobních dat a volný pohyb takových dat (implementace 24/10/98).
- *96/9/EC:* Právní ochrana databází.
- *97/66/EC:* Zpracování osobních dat a ochrana soukromí v telekomunikačním sektoru.
- Doporučení Rady Evropy o ochraně medicínských dat, přijato 13. února 1997.

Zdravotničtí pracovníci, kteří přijdou do styku s osobními daty, jsou osobně zodpovědní za zabezpečení soukromí pacientů. Spolehlivá identifikace pracovníků ve zdravotnictví, kteří s takovou dokumentací přicházejí do styku, je tedy nezbytná před udělením přístupu k citlivým údajům. Požadavek na účinnou ochranu zdravotní dokumentace při zachování jejího širokého využití pro kontinuitu léčebné péče, plánování a výzkum je naléhavý. Stejně důležité, ale poněkud méně uznávané, jsou požadavky na to, aby zdravotní dokumentace, přenášená či ukládaná v digitálním tvaru, byla legislativně považována za rovnocennou její papírové formě. Často jsou výhody

ICT snižovány tím, že je požadováno připojení podpisu na papír. V současné době je klíčovou úlohou dokončit řešení, která umožní, aby se digitálnímu podpisu mohlo věřit stejně, nebo i více než doposud užívanému podpisu na papírovou zdravotnickou dokumentaci.

Důsledky využívání nezabezpečených systémů ve zdravotnictví jsou dalekosáhlé. Pacienti mohou být uvedeni do rozpaků nebo sociálně izolováni kvůli odhalení citlivých informací o jejich duševním zdraví, sexuálně přenosných chorobách, genetických poruchách či závislosti na drogách. Lékařská péče o ně může být narušována nepřesnými nebo chybějícími údaji, které jsou důsledkem neautorizované úpravy, selhání systému nebo chyb vzniklých při návrhu programu. Elektronický zdravotní záznam musí být proto vytvořen, zaveden a provozován takovým způsobem, aby možná pravděpodobnost ublížit pacientovi byla co nejmenší. Většina odborných etických institucí v Evropě klade zodpovědnost za ochranu pacientova záznamu na lékaře vykonávající službu. Například ve Spojeném království Velké Británie a Severního Irska prohlašuje *Všeobecná rada lékařů*: Lékaři nesou primární zodpovědnost za ochranu informací jim svěřených ze strany pacientů, nebo získaných s důvěrou pacientů. Proto musí být přijata opatření, aby se až do výše svých pravomocí ujistili, že záznamy, pořizované ručně nebo počítačem, které přechovávají nebo přenášejí, jsou chráněny účinnými bezpečnostními systémy za použití odpovídajících postupů, které zabrání možnému zneužití.

Podobná prohlášení jsou vydávány odbornými institucemi i v jiných evropských zemích. Pokud však budou programy zpracovávající elektronické záznamy správně vytvořeny, bude možné kontrolovat přístup k nim důkladněji, než je to možné v současnosti s obvyklým manuálním způsobem ukládání a zpracovávání. Zavedení elektronických záznamů nabízí tak možnost vyhovět lépe etickým nárokům a respektovat právo jedince na soukromí a současně neomezit přístup k informacím, které potřebují lékaři. Osobní zdravotní údaje pro účely výzkumu se musí získávat pouze se souhlasem pacienta. Hlavní výhodou především elektronických zdravotních záznamů je pak možnost zpracovávat velké množství anonymizovaných údajů pro potřeby klinického výzkumu.

Velmi důležitý je nedávný vývoj v legislativní oblasti ČR. Prvním je zákon č. 101/2000 Sb. o ochraně osobních údajů. Smyslem zákona o ochraně osobních údajů

je Listinou základních práv a svobod garantovaná ochrana soukromí občana, které je v současnosti vlivem rozvoje informačních technologií stále více narušováno. Druhý zákon je zákon č. 227/2000 Sb., o elektronickém podpisu. Sněmovna schválila zákon č. 260/2001 Sb., který nemocnicím i lékařům umožňuje vést zdravotnickou dokumentaci, pouze na paměťových médiích, pokud zápis zdravotnické dokumentace budou provádět za těchto podmínek:

a) všechny samostatné části zdravotnické dokumentace obsahují zaručený elektronický podpis osoby, která zápis provedla, podle zákona č. 227/2000 Sb., o elektronickém podpisu,
b) bezpečností kopie datových souborů jsou prováděny nejméně jednou za pracovní den,
c) po uplynutí doby životnosti zápisu je zajištěna jejich archivace,
d) uložení archivních kopií, které jsou vytvářeny nejméně jedenkrát za rok, je provedeno způsobem znemožňujícím do nich provádět dodatečné zásahy.

Při uchovávání archivních kopií dat na paměťových médiích musí být zajištěn přístup k datům a jejich čitelnost nejméně po dobu, která je předepsaná pro archivaci zdravotnické dokumentace. Tento krok vede k předpokladu, že rychlý vývoj elektronické zdravotní dokumentace a telemedicíny bude v příštím desetiletí reálný.

Věcným cílem programu Zdravotnictví on-line je zavést nové ICT technologie do zdravotnictví České republiky ve třech následujících okruzích, z nichž jeden ukládá zavést do ordinací a nemocnic možnost vedení pouze elektronické formy záznamu o zdravotním stavu pacientů a připravit plošné zavedení technologie pro používání zaručeného elektronického podpisu při ochraně osobních údajů pacientů. Základním koncepčním dokumentem pro zpracování programu Zdravotnictví on-line je jeho zařazení do Akčního plánu realizace státní informační politiky. Program byl schválen Radou vlády pro státní informační politiku. Koordinací a realizací programu bylo pověřeno Ministerstvo zdravotnictví. Jednotlivé části programu Zdravotnictví on-line jsou zařazeny do materiálu Ministerstva zdravotnictví ČR, ve kterém jsou vymezeny strategické projekty resortu zdravotnictví v oblasti zdravotnické informatiky pro následující období.

3 Analýza současného stavu

V této kapitole uvádím úplnou analýzu současného stavu v jedné z poboček rozsáhlé zdravotnické organizace (viz vymezení cíle práce). Tato analýza bude poté využita v další kapitole k tvorbě návrhu opatření k nejproblematičtějším rizikům, tvorbě bezpečnostní příručky a také tato dokumentace (obzvláště část o fyzické bezpečnosti) bude sloužit jako podklad plánované rekonstrukce prostor vybrané pobočky. Předmětem analýz bude pouze část firmy a údaje o bezpečnosti informací společnosti jako celku nebudou tedy úplné.

3.1 Základní údaje o společnosti

Jak již bylo uvedeno v první kapitole této práce, vybraná společnost nechtěla být jmenována, a proto zde uvedené informace jsou zavádějící.

Obchodní firma:	XYZ, s.r.o.
IČ:	12345678
DIČ:	CZ 1234567890
Sídlo:	město A, Ulice, č. p. 1
Právní forma:	společnost s ručením omezeným
Velikost firmy:	celkem 20 poboček à cca 30 zaměstnanců
Roční obrat:	cca 1,3 mld. Kč

Předmět a rozsah činnosti:
výroba, obchod a služby neuvedené v přílohách 1 až 3 živnostenského zákona
poskytování zdravotní péče

Klasifikace ekonomických činností – CZ-NACE:
86220: Specializovaná ambulantní zdravotní péče
46900: Nespecializovaný velkoobchod
8690: Ostatní činnosti související se zdravotní péčí

Pro naši potřebu budeme používat údaje, okolnosti a data pouze z jedné z dvaceti poboček umístěné v městě B. Tato pobočka je s centrálou spojena pomocí internetu,

přes který putují nejen všechna pacientská data, ale i ostatní důležité firemní dokumenty. Tento způsob představuje nejedno bezpečnostní riziko, ale jiným způsobem toto řešit není možné kvůli centralizovanosti a způsobu řízení celé firmy.

3.2 Situační analýza

Sídlo vybrané pobočky společnosti leží v pronajatých prostorách areálu nemocnice jednoho nevelkého okresního města (cca 25 000 obyvatel) na rozloze cca 600m^2. Celý areál nemocnice je oplocen, a přístup do něj je možný pouze přes hlavní hlídanou vrátnici, hlídaný vjezd na parkoviště, nebo skrz přes den otevřený postranní vchod, určený dříve pro vstup do lékárny, nyní však nevyužívaný, ale nezabezpečený. Areál tedy není dokonale zabezpečený proti přístupu cizích osob a je potřeba se dále věnovat zabezpečení firemních prostor. Prostory jsou situovány v jedné budově v prvním poschodí s přilehlým parkovištěm. Budova nemá více pater. Přístup do samotných prostor je pod kamerovým dohledem a pod ochranným prvkem dveří bez kliky, lze vstoupit jen po osobní kontrole.

Zabezpečení prostor

Ochrana objektu je zabezpečována:

- režimovými opatřeními včetně způsobu přijímání návštěv
- mechanickými zábrannými prostředky – kování na dveřích typu koule
- kamerovým systémem

Na druhé straně prostor je ještě přístup přes požární schodiště na balkón (nouzový vchod), který se však v normálním provozu nepoužívá. Tento přístup není chráněn kamerovým systémem.

Fyzická ostraha (ochranka) v celém areálu nemocnice i v perimetru pobočky firmy chybí, tudíž není možnost zabránit osobám podnapilým a osobám, které by z jiných důvodů mohly ohrozit zdraví a život zaměstnanců nebo jiných osob, způsobit škodu na majetku nebo jinak narušovat pořádek v budově. Po vstupu osoby do objektu požádá zdravotní sestra o identifikaci a důvod návštěvy. Takže jediným platným mechanismem pro odhalení a pro zabránění bezpečnostních incidentů je instalovaný kamerový systém s nastavením nahrávání po dobu 72 hodin.

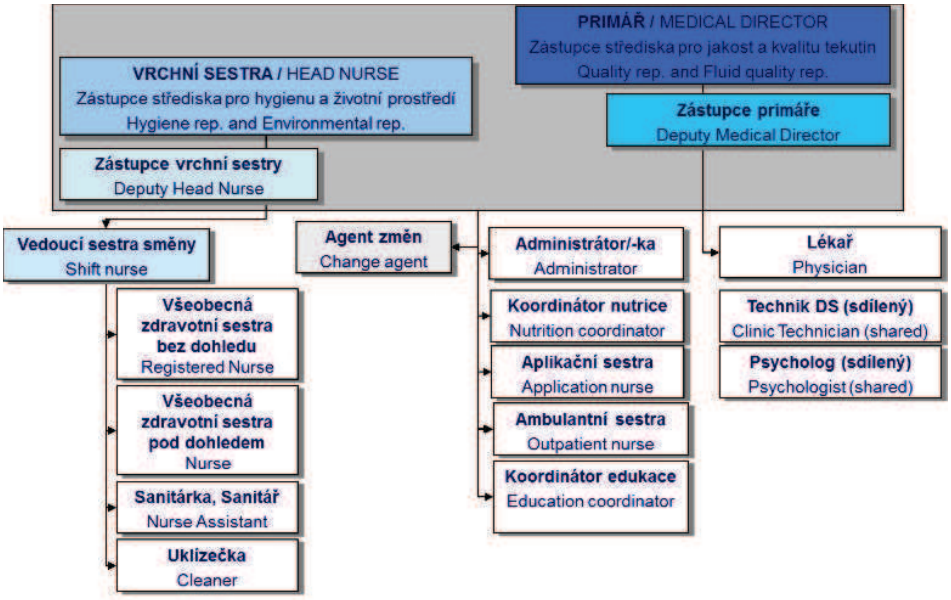
Celkově jsou prostory zastaralé, chybí zde požární hlásiče, jsou pouze vybaveny hasicími přístroji. Personál je pravidelně školen v oblasti protipožární ochrany.

3.3 Personální situace v podniku.

3.3.1 Organizační struktura

Organizační struktura naší vybrané pobočky společnosti XYZ s.r.o. je vyobrazena na následujícím obrázku:

Obrázek 6 Organizační struktura, Zdroj: směrnice firmy (upraveno)



Středisko zaměstnává 27 osob, z nichž převážnou většinu tvoří zdravotní sestry. Jsou přijímány pouze sestry zkušené s praxí na akutních lůžkách nemocnice. Tým lékařů tvoří vysoce kvalifikované osoby s patřičnými zkušenostmi. V čele střediska stojí vedoucí lékař. Ten zodpovídá za veškeré dění na středisku. Další personál tvoří specialisti v odborných oblastech, např. sestra určená pro výživu pacientů, aplikační sestra, která zavádí nové pracovní postupy a technologie, a edukační sestra, která se stará o poučování pacientů v problematice jejich nemoci. Pomocný personál střediska tvoří sanitáři a uklízečky. Externí personál zajišťuje technickou podporu zdravotních přístrojů. Tým má také k dispozici externího psychologa. V problematice IT na středisku je zaměstnána středoškolsky vzdělaná administrátorka, která má za úkol

koordinovat činnost střediska s centrálou v oblasti informatiky, statistiky a styku s pojišťovnami. V IT oddělení v centrále pracují vysokoškolsky i středoškolsky vzdělaní lidé, kteří zabezpečují správné fungování sítě a všech informačních technologií. Za strategická rozhodnutí je zodpovědný management firmy působící v centrále.

Při vstupu do zaměstnání podepisují noví pracovníci smlouvu o mlčenlivosti, která jasně definuje vztah mezi zaměstnanci a pacientem, zaměstnanci a firmou a také sankce při porušení smlouvy.

3.4 Informační situace v podniku

Jako klientský operační systém je zaveden Microsoft Windows XP Professional. V podniku se nachází dvanáct koncových počítačů včetně jednoho notebooku, na kterých se zpracovávají informační aktiva společnosti a pacientská data. Co se týká připojení počítačů do sítě, žádná stanice není připojena pomocí modemu, ale všechny mají standardní síťové konektory RJ-45. Na polovině počítačů jsou dokonce síťové přípojky dvě. Jedna je standardně pro komunikaci přes internet s centrální databází a druhá je pak pro připojení do interní sítě nemocnice. Z pohledu manipulace s daty či datovými nosiči včetně USB Flashdisků nepodléhají systémy žádnému omezení. Co se týká antivirové ochrany, je zde provedeno serverové řešení, kdy se aktualizace virové databáze automaticky zavádí přímo na koncové stanice centrálně. Antivirový program je od firmy ESET, jmenuje se NOD32. Pro administrativní úkony a mail je zavedeno prostředí Lotus Notes, které implementuje i kalendář a databázi interních informací včetně zápisů ze schůzí a interních směrnic. Toto prostředí má zabudovánu ochranu proti spamu pomocí blacklistů (seznamů) spamových adres. Většina uživatelských účtů má práva lokálního administrátora. Tím pádem může každý uživatel volně stahovat a instalovat jakýkoliv software. Pouze aktualizace operačního systému jsou stahovány centrálně a distribuovány na jednotlivé stanice, aby se omezil síťový provoz. V areálu je využita i bezdrátová technologie WiFi sítě. Díky WiFi technologii mají možnost připojení k internetu také pacienti. Každá osoba musí pro přístup do bezdrátové sítě obdržet heslo. Síť je chráněna pomocí technologie WPA2 (Wi-Fi Protected Access 2).

3.4.1 Hardwarové vybavení pobočky

Na středisku je celkem jedenáct koncových PC, jeden notebook a jeden server. Většina z pracovních počítačů je značky OptiPlex 790 nebo OptiPlex 780 od firmy Dell. Tato řada běžně obsahuje 4GB RAM, procesor Intel Core i5-2500@2,7GHz a 260GB HDD Seagate. Notebook je z řady Dell Latitude D630, která obsahuje 2GB operační paměti, procesor Intel Core 2 DUO@2GHz a 120GB HDD 7200RPM. Operační systém zde zastupuje systém Microsoft Windows XP Professional, až na dva pracovní počítače, kde je nasazen Microsoft Windows 7 Professional, a server s řešením Microsoft Windows Server 2008 Standard. Server má vlastní záložní zdroj (UPS) umožňující zhruba dvacetiminutový chod v případě výpadku dodávky elektrické energie. Server je automaticky nakonfigurován tak, aby se v případě přechodu na záložní zdroj přivedl k bezpečnému ukončení provozu.

3.4.2 Softwarové vybavení

Základní informační systém, který je využívaný v celé organizaci, je řešen pomocí firemního programu fungujícího v celodenním provozu pomocí připojení přes internet. Tento systém vystřídal původní, který přestal vyhovovat specifickým požadavkům firmy. IT oddělení reagovalo na tuto situaci vývojem své vlastní aplikace, a tím došlo k zásadní změně práce lékařů a sester. Změnilo se i úložiště dat, které se z lokálního serveru přestěhovalo do centrálních kanceláří firmy mimo prostory pobočky. Tím se nově začalo využívat vnějších komunikačních tras. V tomto případě jde o systém provozovaný mimo síť organizace.

Pomocné a administrativní informační systémy se skládají z několika komerčních a několika vlastních programů. Mezi komerční patří například Microsoft Office 2003, docházkový systém PowerKey, komunikační a emailový program Lotus Notes a nemocniční informační systém Medicalc. Vlastní programy z důvodu ochrany firemního tajemství zde nebudu uvádět.

3.5 Analýza rizik

Na základě rozhovoru s vedoucím lékařem na středisku byla provedena analýza rizik dle pravidel popsaných v kapitole 2.4 této práce – Analýza rizik. Nejprve byla identifikována dostupná aktiva, bylo provedeno jejich ohodnocení a následně identifikace hrozeb a zranitelností systému informací.

3.5.1 Identifikace aktiv

Aktiva byla rozdělena do následujících kategorií dle logické návaznosti:

- DATA
- ORGWARE (pravidla fungování)
- SOFTWARE
- HARDWARE
- SLUŽBY

Každá z těchto kategorií se pak člení do skupin aktiv a je jim přiřazena lokalita, kde se vyskytují.

Vše dokumentuje názorná tabulka níže:

Tabulka 2 Identifikace aktiv, Zdroj: vlastní tvorba

Kategorie aktiv	Aktivum	Umístění
DATA	Lékařská dokumentace - elektronická	Vzdálený server
	Lékařská dokumentace - papírová	Vlastní pracoviště
	Osobní údaje personálu	Vzdálený server, vlastní pracoviště
	Faktury zdravotním pojišťovnám	Vzdálený server, vlastní pracoviště
ORGWARE	Interní směrnice	Vzdálený server, vlastní pracoviště
	Docházkový systém	Vzdálený server
SOFTWARE	Zdravotnický software	Vzdálený server
	Technický software	Server pracoviště
	Operační systémy	Koncové stanice
HARDWARE	Server	Vzdálené i vlastní pracoviště
	Koncové stanice - 7 PC	Vlastní pracoviště
	Periferie - tiskárny, čtečky pac. karet, scanner	Vlastní pracoviště
	Síťové prvky	Vlastní pracoviště
SLUŽBY	Komunikační trasy	Vzdálené i vlastní pracoviště
	Základní služby (světlo, topení, klimatizace)	Vlastní pracoviště

3.5.2 Ohodnocení aktiv

Druhým krokem analýzy rizik je ohodnocení aktiv. Metodika je popsána v teoretické části práce. Po diskuzi s vedoucím lékařem vznikla následující tabulka ohodnocení aktiv:

Tabulka 3 Ohodnocení aktiv, Zdroj: vlastní tvorba

Aktivum	Dostupnost	Důvěrnost	Integrita	Hodnota
Lékařská dokumentace - elektronická	5	5	5	5
Lékařská dokumentace - papírová	2	5	4	4
Osobní údaje personálu	2	5	3	3
Faktury zdravotním pojišťovnám	2	3	4	3
Interní směrnice	3	4	4	4
Docházkový systém	4	3	5	4
Zdravotnický software	5	5	5	5
Technický software	3	4	4	4
Operační systémy	5	5	5	5
Server	5	5	5	5
Koncové stanice - 7 PC	3	5	4	4
Periferie - tiskárny, čtečky pac. karet, scanner	2	2	3	2
Síťové prvky	5	5	5	5
Komunikační trasy	5	5	5	5
Základní služby (světlo, topení, klimatizace)	4	1	3	3

Z této tabulky vyplývá, že jako nejcennější aktiva byly identifikovány tyto:

- Elektronická lékařská dokumentace
- Zdravotnický software
- Operační systémy
- Server
- Síťové prvky
- Komunikační trasy

Na ně se v dalším zkoumání zaměřím více.

3.5.3 Identifikace hrozeb a zranitelností

Po detailní analýze rizik pomocí dvou parametrů jsme dospěli k těmto hrozbám a zranitelnostem, ze kterých ty nejvýznamnější přesněji popíši. Rizika jsou rozdělena podle aktiv, kterým jsou přímo vystavena. Popisovat všechna rizika a dělat komplexní analýzu by bylo nad rámec této diplomové práce.

3.5.3.1 Lékařská dokumentace – elektronická

Jedním z nejdůležitějších nehmotných aktiv ve zdravotnické organizaci jsou právě data pacientů. Nad touto skupinou aktiv jsem identifikoval následující hrozby a k nim patřící zranitelnosti. Nedodržování lékařských postupů a směrnic vede k špatně stanoveným případně špatně zapsaným diagnózám v dokumentaci pacientů. Tento problém může též nastat, když je lékař unaven nebo pod nějakým stresem, což souvisí s nevhodnými pracovními podmínkami při výkonu léčby (více viz dále). Dále hrozí například ztráta dat při nesprávném postupu a nedostačujících kontrolách pravidelného zálohování nebo při napadení informačního systému virem a nasazení jiných destruktivních programů. Při špatném fyzickém zabezpečení prostor hrozí krádež datového úložiště. Lékařská dokumentace může být zcizena i skrze internetové připojení při nabourání se cizími silami do informačního systému nebo do komunikační trasy, přes kterou tyto data putují. Po krádeži je dalším rizikem zneužití těchto dat. Únik informací hrozí také ze strany autorizovaných uživatelů informačního systému. Toto by mělo být podchyceno skrze oblast bezpečnosti z hlediska lidských zdrojů.

3.5.3.2 Lékařská dokumentace - papírová

Pro účely kontrol a archivace se zálohují data pacientů také na papír do tzv. kartoték, což je vlastně duplicita předešlé kategorie, ale to je na rozdíl od elektronických dat hmotné aktivum a nehrozí mu tak závažná rizika, protože lze snadno data dotisknout z databáze do této podoby. Papírová dokumentace slouží především k předkládání během auditů či kontrolám ze strany zdravotních pojišťoven a jako podklady k soudním jednáním. Velký důraz je potom kladen na jejich zničení, aby nebylo možno jich zneužít. Poté, co byla data zneplatněna nebo jiným způsobem již nejsou na pracovišti potřeba, je nutno je řádně skartovat podle skartačního řádu a nevyhazovat do odpadu s ostatním papírem. Rizika s nimi spojená jsou obdobná jako v předešlé kategorii, jen se zde může identifikovat několik odlišností. Nedají se tak jednoduše zálohovat jako data

v elektronické podobě, a tudíž je potřeba je archivovat ve speciální místnosti s dobrým zabezpečením. Hrozí jim riziko poškození při požáru nebo při vyplavení vodou. Všechny informace o pacientech by měly být klasifikovány jako důvěrné a podle toho by se s nimi také mělo zacházet.

3.5.3.3 Osobní údaje personálu

Dalším souborem aktiv jsou osobní údaje personálu, které podléhají nařízení zákona o ochraně osobních údajů, a je nezbytné s nimi takto nakládat. V našem případě jsou jak v elektronické podobě na serveru v centrále, tak v papírové podobě na pobočce pro účel kontrol. Jsou vystaveny rizikům krádeže a zneužití dat. Proto by měly být správně zabezpečeny, abychom se nevystavovali rizikům odhalení citlivých osobních informací.

3.5.3.4 Faktury zdravotním pojišťovnám

Faktury zdravotním pojišťovnám jsou základním zdrojem příjmu celé firmy. Je jím věnována mimořádná pozornost, proto jsou hlavní náplní práce administrátora v každé pobočce firmy. Koordinaci údajů z faktur obstarává vlastní softwarový produkt modul pojišťovna. Tento program vygeneruje ze zdravotnických výkonů podklady pro fakturaci zdravotním pojišťovnám. Tyto podklady jsou přeneseny přes internet do centrální účtárny, která fakturuje pojišťovnám pomocí jejich webových portálů. Během tohoto procesu hrozí několik rizik. Nejrizikovější je chyba při kontrole zpracování dat administrátorem pobočky. Dalšími riziky jsou poškození centrálního serveru před odesláním do pojišťoven, nebo lokálního datového úložiště před odesláním do centrály. Málo pravděpodobným rizikem je pak odposlech při přesunu přes síť internet, proti čemuž se lze bránit účinným šifrováním dat.

3.5.3.5 Interní směrnice

Interní směrnice jsou významným nehmotným majetkem firmy a neměly by se dostat do rukou nepovolaným osobám nebo konkurenci. V těchto směrnicích jsou zapsány a detailně vysvětleny jednotlivé kroky a pracovní postupy při konkrétních situacích, jednotlivé role a odpovědnosti zaměstnanců a zároveň také zabezpečení IT infrastruktury, bezpečnosti bezdrátové sítě apod. Je zde popsána firemní strategie, vize, cíle a know-how společnosti. Kdyby se vyzradily tyto směrnice, mohlo by se jednat o zvýšení rizika pro danou pobočku z pohledu vnějšího útoku.

3.5.3.6 Docházkový systém

Docházkový systém je souborem dat důležitý při rozhodování o výši mzdy a přidělování dovolené. Je to důležitý svazek informací o příchodech a odchodech zaměstnanců, jehož integrita by neměla být porušena. Jinak hrozí nepořádek v dalším systému organizace, ohrožuje vlastní provoz střediska a při vnitřních auditorských kontrolách jsou za chyby v systému uplatňovány sankce. Proto je důležité tento systém udržovat v bezpečném režimu, kdy nehrozí ani ztráta dat, ani jejich vyzrazení či zneužití. Také udržování systému v chodu je důležité, neboť při nefunkčnosti by zaměstnanec mohl přijít o značnou část své mzdy.

3.5.3.7 Zdravotnický software

V kategorii SOFTWARU je nejrizikovější skupina zdravotnických programových vybavení, kdy je třeba hlídat nejen jeho zabezpečení proti ztrátě, úniku, zcizení a následnému zneužití dat, se kterými aplikace pracují. Důraz je kladen také na integritu a dostupnost těchto medicínských dat, protože právě fakt, že lékaři potřebují správná data včas, je obzvláště důležitý. Žádný software není bezchybný, z čehož vyplývá, že celý systém nasazování a implementace zdravotnického softwaru do provozu není jednoduchý ani rychlý. Vše je potřeba řádně otestovat a často aktualizovat podle potřeb a vývoje ve zdravotnictví. V našem případě jsou hlavní aplikace dostupné přes veřejné sítě na firemním serveru, kde uživatel programu používá pouze tzv. tenký klient (například webový prohlížeč) nebo klientskou verzi aplikace. Toto řešení přenáší téměř všechna rizika na stranu, kde je provozován mateřský server. Zároveň je třeba podchytit komunikační vazby, přes které data putují. Problémem může být i nedostatečná funkčnost programu, která dále zdržuje výkony lékařských zaměstnanců. Důsledkem nedostatečného školení v této oblasti může být nevyužívání všech funkcí softwaru a tím pádem další prodlužování léčebné procedury. Existují zde lidské neúmyslné hrozby, kdy problémem je například neukládání práce průběžně. Další hrozbou je chybná manipulace s uživatelskými účty, kdy se jeden lékař neodhlásí a jiný pracuje pod jeho identitou. Toto jsou však již požadavky na konkrétní aplikaci v konkrétním prostředí. V neposlední řadě existuje také riziko zneužití firemních aplikací a dat z nich při jiné praxi než ve výkonu zaměstnání. Tím se však již porušují smluvní podmínky o mlčenlivosti v zaměstnaneckém úvazku. Jedná se zde o tzv. vnitřní úmyslný útok.

3.5.3.8 Technický software

Tato kategorie je označena právě takto, protože se do ní dají zahrnout všechny podpůrné programy, jako jsou kancelářské balíky, programy pro zpracování docházkového systému, programy pro řízení a provoz lékařských přístrojů a programy pro komunikaci se zdravotními pojišťovnami. V případě neaktualizovaných kancelářských balících hrozí celému systému napadení virem, následná ztráta dat a všechny důsledky s tím spojené. Platí zde stejné podmínky jako u zdravotnického softwaru při nedostatečném školení a nedostatečné funkčnosti.

3.5.3.9 Operační systémy

Kategorie operačních systémů je důležitá z pohledu provozování dalších aplikací nad touto vrstvou. Nad ní fungují všechny konkrétní programy, a proto je na místě, aby cílové počítače měli plně aktualizovaný a i dále aktualizovatelný operační systém. V tomto případě je dobré připomenout, že veškerá podpora všech verzí operačního systému Microsoft Windows XP byla ke dni 8. 4. 2014 ukončena. To znamená, že již nadále nebudou poskytovány aktualizace a bezpečnostní opravy tohoto operačního systému a je nutno přejít na operační systém s vyšší úrovní zabezpečení jako např. Microsoft Windows 7. Tento však klade již větší nároky na použitý hardware, což by mohlo znamenat nutnost zakoupení nebo minimálně upgradu nových koncových zařízení (PC) a velice se prodražit. Další alternativou by bylo sáhnout po bezplatném opensource operačním systému na bázi GNU/Linux (např. některé verze XUbuntu), kterým tolik nehrozí zavirování a jiné klasické bezpečnostní hrozby. Bohužel však většina aplikací používaných ve zdravotnictví určených pro architekturu MS Windows není kompatibilní s tímto operačním systémem a musely by se pro tuto novou architekturu překompilovat. Ve výsledku by toto řešení pak mohlo vyjít ještě dráž.

3.5.3.10 Server

Nejkritičtější skupinou hmotného majetku a součástí IS ve zdravotnictví jsou servery. Uchovávají důležité lékařské informace a starají se o převážnou část chodu aplikací, jejich zabezpečení apod. Na jejich ochranu a opatření proti poškození či zcizení by měl být kladen největší důraz. Servery se umísťují do tzv. serverovny, což je speciální místnost s podmínkami, které zabezpečují správný chod těchto serverů. Tato místnost by měla být zajištěna jak proti přírodním katastrofám (požár, zatopení, zemětřesení

apod.), tak proti vnějšímu i vnitřnímu útočníkovi. V naprosté většině případů bývá umístěna ve vyšším nadzemním podlaží právě kvůli snížení pravděpodobnosti vyplavení a následného znehodnocení komponent serverů. Měla by být vybavena systémem protipožární ochrany. Neměly by zde být ani vyústěny ani vedeny žádné vodovodní ani odpadní toky. Dále by měl být zajištěn náhradní zdroj energie v podobě výkonné UPS (Uninterruptible Power Supply) pro případ, kdyby došlo k výpadku elektrické energie. Ve zdravotnictví však jsou nároky na zajištění elektrické energie ještě vyšší, takže standardním vybavením by měl být i motorgenerátor uzpůsobený na dodávku energie alespoň po dobu 48 hodin. Serverovna by neměla být přístupná komukoliv, měla by být vybavena bezpečnostním zámkem a je vhodné zavést systém záznamu, kdo místnost kdy a proč navštívil.

3.5.3.11 Koncové stanice

Koncovými stanicemi rozumíme počítače (PC) a notebooky, popřípadě tablety a jiná výpočetní a zobrazovací zařízení. Tyto slouží ve zdravotnických organizacích buďto jako zobrazovací terminály, pomocí nichž se lékaři připojují na mateřský server s daty a data mohou číst, měnit a mazat. Nebo mohou v menších ordinacích, kde není nutno vlastnit samostatný server, zastupovat samotné úschovny (databáze) pacientských informací. Pokud slouží pouze jako zobrazovací terminály, není nutno klást takové nároky na jejich fyzické zabezpečení jako v případě serverů, ale je potřeba zavést bezpečnostní směrnice ohledně přístupu na síťovou infrastrukturu, k serverovým datům a celkové manipulaci skrze uživatelská práva. Nemálo důležitým krokem by mělo být zvážení a omezení tzv. politiky BYOD (Bring Your Own Device), což je ve zkratce povolení přístupu a práce lékařů a zaměstnanců na svých koncových zařízeních, jejž si donesou z domova. Samozřejmostí zde je návaznost a propojenost jak s riziky operačních systémů, tak s riziky zdravotních a technických aplikací.

3.5.3.12 Periferie – tiskárny, čtečky pacientských karet, scannery

Asi nejméně kritickým aktivem je kategorie periferních zařízení, jež pouze dopomáhají k rychlosti celého systému léčby. Zde bych zmínil, že je potřeba kontrolovat správnou funkčnost tiskáren, kopírek a skenerů. Protože například minulý rok byla objevena chyba kopírek značky Xerox, která způsobila záměnu jistých číslic v kopiích

dokumentů [12], což by mohlo mít fatální důsledek například na výsledky rozboru krve při lékařské péči.

Dále je třeba kontrolovat funkčnost čteček pacientských karet a vlastních pacientských karet, protože v případě poškození, ztráty či záměny se výrazně ovlivní léčebný proces pacienta.

3.5.3.13 Síťové prvky

Klíčová kategorie pro komunikační zabezpečení je právě kategorie síťových prvků. Přes tyto zdánlivě nedůležitá aktiva směřuje velké množství pacientských dat jak po vnitřní síti ze serveru do zobrazovacích zařízení, tak po venkovní síti přes internet, pokud jsou servery umístěny např. v jiném městě. Jejich zabezpečení je kritické i z pohledu zabezpečení pasivní vrstvy. Konkrétně se jedná o úmyslnou manipulaci personálu s konektory, neúmyslnou manipulaci uklízečkou při úklidu, úmyslné poškození kabelů cizí osobou, neúmyslné poškození kabelů údržbářem při opravě jiného vybavení.

3.5.3.14 Komunikační trasy

Jako další aktivum si představíme vnější komunikační trasy. Toto aktivum nenáleží vybrané zdravotní společnosti, ale organizace je na něm přímo závislá. V dnešním světě jsou počítačové sítě tak provázané, že je těžké určit, kde má útok svůj zdroj. Při putování dat přes internet hrozí rizika přerušení trasy nebo odposlechu, a proto je zapotřebí data přenášená vnější sítí zašifrovat a ochránit tak proti těmto možným útokům.

Dále zde hrozí riziko tzv. blackoutu neboli výpadku jedné z komunikačních tras, a proto je zapotřebí poskytované služby zdvojovat a co nejlépe tak zachovat dostupnost nejen pacientských dat.

K infiltraci elektronické komunikace dochází, když jednotlivec (například hacker) falšuje normální tok dat v síti. Nejčastějším důsledkem je útok typu odmítnutí služby (ve kterém dojde k účinnému odstavení serverů nebo sítových zdrojů), ale může dojít i k jiným formám infiltrace (například útok opakovaného přehrání, kdy je platná, ale zastaralá zpráva opakovaně přenášena tak, aby udělala dojem, že je nová). Infiltrace komunikací představuje selhání detekce průniku, a/nebo řízení přístupu k síti, a/nebo analýzy rizik (zvláště analýzy zranitelnosti), a/nebo architektury systému (který je potřeba navrhnout s obranou proti útokům typu odmítnutí služby).

Pokud nejsou zprávy během přenosu zašifrovány, může dojít odposlechem komunikace k porušení důvěrnosti informací obsažených ve zprávě. Je to jednodušší, než to vypadá, protože kdokoliv přihlášený k místní síti může nainstalovat takzvaný „packet sniffer“ na svou pracovní stanici a sledovat velkou část sítového provozu na své lokální síti včetně čteni e-mailů během jejich přenosu. Nástroje hackerů pro automatizaci a zjednodušení velké části tohoto procesu jsou snadno dostupné. Odposlech komunikací představuje selhání v bezpečných komunikacích.

Tato hrozba zahrnuje uživatele, kteří popírají, že by poslali zprávu (popření původu) a uživatele popírající, že zprávu obdrželi (popření přijetí). Jednoznačné stanovení, jestli osobní zdravotní informace byla přenesena od jednoho uživatele ke druhému, je zásadním rysem vyšetřování lékařského zneužiti pravomoci. Popření může znamenat selhání při aplikaci opatření, jako jsou digitální podpisy na elektronických předpisech (příklad popření původu) nebo opatření, jako je oznámení o přečtení emailových zpráv (případ popření přijetí).

Selháni připojení (včetně selhání sítí zdravotnických informací). Všechny sítě jsou náchylné k výpadkům služeb. Kvalita služby je hlavním faktorem poskytováni síťových služeb ve zdravotní péči. Selhání připojení může také vyplývat ze špatného nasměrování síťových služeb (například úmyslná změna routovacích tabulek, která způsobí přesměrování provozu v síti). Selhání propojení může usnadnit vyzrazení důvěrných informací tím, že donutí uživatele poslat zprávy méně bezpečným mechanismem, jako třeba faxem nebo přes internet.

3.5.3.15 Základní služby (světlo, voda, teplo, klimatizace, zabezpečení pracoviště)

Základní zranitelnosti pobočky organizace pro tuto kategorii zastupují hlavně nedostatečné zabezpečení proti živelným pohromám, staré rozvody vody, odpadu a elektrické energie, umístění elektrických rozvaděčů na místech přístupných běžné veřejnosti a také zde vystupuje lidský faktor v podobě neúmyslného zapomenutí zabezpečení objektu (nutno zavřít všechna okna a zamknout dveře), nebo úmyslná sabotáž bezpečnosti. Pokud není pracoviště řádně zabezpečeno vůči cizím osobám, hrozí riziko vloupání, krádeže nebo i zničení vybavení pracoviště.

Na tomto místě se nesmí opomenout špatné pracovní podmínky zaměstnanců společnosti, jako jsou nepřiměřené osvětlení, teplotní zázemí nebo ergonomie a rozmístění užívaného vybavení pracoviště. Tento poslední bod se zdá být pro bezpečnost již irelevantní. Avšak v lékařské praxi, kde je bohužel většinou málo pracovníků, je potřeba maximální komfort pracujících lékařů, neboť pokud jsou tito vyčerpaní nebo pod jakýmkoliv stresem, je jejich léčba chybová a pro subjekt péče to může vyústit v onemocnění, zranění či smrt z nesprávně stanovené léčby.

4 Vlastní návrhy řešení

V této kapitole uvádím informace o bezpečnostní politice při nasazování ISMS do zdravotnické organizace. Dále jsem vypracoval bezpečnostní příručku, což je soubor navrhovaných opatření ke zmenšení rizik plynoucí z dřívějších analýz aplikovatelných obecně pro pobočku zdravotnické organizace. V závěru kapitoly navrhuji zavedení nových bezpečnostních směrnic na základě bezpečnostní příručky pro vybranou firmu a také navrhuji zavádění ISMS do celé organizace na základě tabulek se zdroji, odpovědnostmi a harmonogramy zavádění opatření.

4.1 Bezpečnostní politika

Prvním krokem nasazování ISMS je definovat směr a vyjádřit podporu bezpečnosti informací ze strany vedení v souladu s požadavky organice, příslušnými zákony a regulatorními požadavky.

Vedení organizace by mělo stanovit jasný směr postupu v oblasti bezpečnosti informací, ukázat její podporu vydáním a aktualizací bezpečnostní politiky informací platné v celé organizaci. Dokument bezpečnostní politiky informací by měl být schválen vedením organizace, vydán a dán na vědomí všem zaměstnancům a relevantním třetím stranám. Dokument by měl obsahovat následující body:

a) definice bezpečnosti informací, její cíle, rozsah a její důležitost - mechanizmus umožňující sdílení informací;
b) prohlášení vedení organizace o záměru podporovat cíle a principy bezpečnosti informací;
c) stručný výklad bezpečnostních zásad, principů a norem a požadavky zvláštní důležitosti pro organizaci, například:
    a. dodržování zákonných, regulatorních a smluvních požadavků;
    b. požadavky na vzdělávání, školení a zvyšování povědomí v oblasti bezpečnosti;
    c. zásady plánování kontinuity činností organizace;
    d. důsledky porušení bezpečnostních zásad;
d) stanovení obecných a konkrétních odpovědností pro oblast řízení bezpečnosti informací včetně hlášení bezpečnostních incidentů.

4.2 Návrhy na opatření proti rizikům – bezpečnostní příručka

Společnost je držitelem certifikátů norem ISO 9001:2008 a ISO 14001:2004, z čehož plyne, že již některé postupy zavedeny má. A to hlavně v oblasti lidských zdrojů. Vzhledem k práci s důvěrnými informacemi by společnost z vlastního zájmu měla usilovat o certifikaci dle normy ČSN ISO/IEC 27001. Účelem bezpečnostní příručky je rozpracovat opatření v oblasti řízení obecné bezpečnosti informací, která jsou vhodná k aplikaci do systému řízení bezpečnosti informací vybrané pobočky společnosti.

Tato příručka popisuje opatření vybraná na základě analýzy rizik v oblastech:

- organizace bezpečnosti informací;
- řízení aktiv;
- bezpečnost z hlediska lidských zdrojů;
- fyzická bezpečnost a bezpečnost prostředí;
- řízení komunikací a řízení provozu;
- řízení přístupu;
- akvizice, vývoj a údržba informačních systémů;
- zvládání bezpečnostních incidentů;
- aspekty řízení kontinuity činností organizace z hlediska bezpečnosti informací;
- shoda s právními požadavky.

4.2.1 Organizace bezpečnosti informací

Vedení zdravotnické organizace je odpovědné za bezpečnost osobních zdravotních informací a jiných chráněných dat. Platí to zvláště pro ty organizace, jejichž řízené služby poskytují třetí strany. Efektivní koordinace je zásadní pro zachování bezpečnosti informací.

Úlohu nejvyššího bezpečnostního orgánu zastává představenstvo celé firmy. Problematiku bezpečnosti informací je zapotřebí pravidelně projednávat na jednáních představenstva, kterého se účastní i bezpečnostní manažer. Jednání představenstva k problematice bezpečnosti informací bude prováděno minimálně 1x za půl roku.

K řízení a koordinaci bezpečnosti informací budou do jednoho měsíce stanoveny následující funkce:

- **Představitel vedení pro ISMS** – odpovědný vedoucímu představenstva za provádění systému řízení bezpečnosti informací.
- **Bezpečnostní manažer** – realizuje bezpečnostní opatření ISMS a navrhuje jejich změny, sleduje dodržování bezpečnostních opatření a provádění jejich změn, ustanovuje hodnocení rizik, řešení bezpečnostních incidentů a zvyšování bezpečnostního povědomí zaměstnanců celé organizace.
- **Bezpečnostní správce sítě** – odpovídá za implementaci a aktualizaci bezpečnostních opatření při správě počítačové sítě celé organizace. Po odborné stránce je podřízen bezpečnostnímu manažerovi. Mezi jeho povinnosti patří agenda týkající se počítačové sítě, přístupových práv uživatelů systému, sledování stavu bezpečnosti počítačové sítě organizace s důrazem na kontrolu a nastavení bezpečnostních parametrů.
- **Vlastníci aktiv** – odpovídají za správu jednotlivých aktiv, pro která jsou zvoleni s důrazem na úplnost a spolehlivosti informací souvisejících se spravovaným aktivem a vymezení pravidel zacházení se spravovanými aktivy.
- **Administrátor** – odpovídá za vlastní nastavování bezpečnostních parametrů jak počítačové sítě, tak prvků infrastruktury, včetně jednotlivých počítačů. Dále odpovídá za antivirovou a protispamovou ochranu počítačové sítě včetně poštovního serveru a rozhraní mezi počítačovou sítí organizace a veřejnou sítí internet.
- **Koordinátor řízení kontinuity činností** – odpovídá za nastavení procesů pro včasnou reakci na stav vyžadující obnovu části nebo celého systému spadajícího do ISMS. Jedná se především o zálohování nejdůležitějších informací a jejich obnovu v nutném případě.
- **Auditor ISMS** – zaměstnanec organizace, který je povolán jako interní auditor ISMS.

4.2.2 Řízení aktiv

Cílem je udržovat přiměřenou ochranu aktiv organizace.

U všech důležitých informačních aktiv bude stanovena odpovědnost a určen jejich vlastník. Pro všechna důležitá aktiva budou určeni vlastníci a bude stanovena jejich odpovědnost za udržování přiměřených bezpečnostních opatření. Odpovědnost za realizaci jednotlivých bezpečnostních opatření může být delegována, ale vlastní odpovědnost za ně zůstane na vlastníkovi aktiva.

4.2.2.1 Odpovědnost za aktiva

Do jednoho měsíce budou identifikována všechna aktiva organizace, všechna důležitá aktiva budou evidována a seznam bude udržován aktuální.

Organizace identifikuje svá aktiva a stanovit jejich relativní hodnotu a důležitost. Evidence bude obsahovat informace potřebné pro případ obnovy po havárii. Bude uveden typ aktiva, jeho formát, umístění, informace o záloze, licenční informace a jeho hodnota pro organizaci. Seznam by neměl zbytečně duplikovat jiné, již existující seznamy. Pokud se tak stane, bude zajištěna shoda uváděných informací. Veškeré informace a aktiva související se zařízením pro zpracování informací budou mít určeného vlastníka (jedinec nebo entita, který má vedením organizace přidělenou odpovědnost za výrobu, vývoj, údržbu, použití a bezpečnost aktiv).

Vlastník aktiva bude odpovědný za:

a) zajištění odpovídající klasifikace informací a aktiv souvisejících s prostředky pro zpracování informací;
b) přesné vymezení a pravidelné přezkoumání omezení přístupu a klasifikace aktiv, v souladu s platnou politikou řízení přístupu

4.2.2.2 Klasifikace aktiv

Cílem klasifikace aktiv je zajištění přiměřenosti ochrany informačních aktiv. Informace budou klasifikovány tak, aby byla naznačena jejich potřebnost, důležitost a stupeň ochrany s ohledem na jejich hodnotu, právní požadavky, citlivost a kritičnost. Tyto postupy musí pokrývat informační aktiva ve fyzické i elektronické podobě. Informace mohou mít různý stupeň citlivosti a mohou být různě kritické, některé mohou vyžadovat vyšší úroveň bezpečnosti nebo zvláštní způsob zacházení. Do dvou měsíců sestaví bezpečnostní manažer systém bezpečnostní klasifikace, který bude určovat adekvátní

stupeň ochrany a který bude dávat uživatelům informace o nutnosti zvláštního zacházení. Odpovědnost za klasifikaci nese vlastník aktiva. V zásadě klasifikace umožňuje rychle určit způsob zacházení s informacemi a způsob jejich ochrany.

Všechny informace organizace budou klasifikovány. Klasifikační stupeň se informaci přiřadí podle významu chráněného zájmu a závažnosti obsahu. Organizace bude jednotně klasifikovat osobní zdravotní data jako důvěrná.

Pro účely klasifikace informací organizace bude zavedeno následující **klasifikační schéma**:

- Interní informace – jsou to informace, které vznikly z činnosti firmy nebo s její činností souvisejí a jejichž vyzrazení, zneužití nebo poškození může být pro organizaci nevýhodné. Interní informace nejsou specificky označovány a jsou distribuovány v rámci firmy bez rozlišení zaměstnanců.
- Důvěrné informace – jsou to informace, které vznikly z činnosti firmy nebo s její činností souvisejí a jejichž vyzrazením či zneužitím mohou být vážně ohroženy zájmy organizace. Patří sem převážně osobní zdravotnická data. Důvěrné informace jsou označovány značkou DŮVĚRNÉ nebo CONFIDENTAL a jsou distribuovány dle rozdělovníku nebo seznamu přístupových práv definovanému okruhu zaměstnanců.

Důvěrnost osobních zdravotních informaci je často převážně subjektivní spíše než objektivní. Jinak řečeno v zásadě pouze datový subjekt (tj. subjekt péče) může náležitě určit relativní důvěrnost různých oborů nebo seskupení dat. Například osoba, prchající před vztahem, který ji ohrožuje, bude považovat svou novou adresu a telefonní číslo za mnohem důvěrnější, než klinické údaje o své zlomené ruce. Důvěrnost osobních zdravotních informaci závisí na jejich kontextu. Jméno a adresu v seznamu osob přijatých na pohotovost nemůže subjekt péče považovat za zvlášť důvěrné, ale v seznamu pacientů přijatých na kliniku zabývající se léčbou impotence budou tato data subjektem hodnocena jako vysoce důvěrná. Důvěrnost osobních zdravotních informací se může během životnosti zdravotních záznamů jednotlivce měnit.

Například vzhledem ke změnám sociálních postojů za posledních dvacet let už mnoho subjektů péče nepovažuje údaje o jejich sexuální orientaci za důvěrné. Naproti tomu údaje o poskytovaných poradenských službách při závislostech na alkoholu

a drogách dnes považují subjekty péče za mnohem důvěrnější, než by je považovali před dvaceti lety. Protože nikdo nemůže předvídat citlivost dané části osobních zdravotních informaci pro všechna její použití a fáze životního cyklu, měly by všechny osobní zdravotní informace vždy podléhat pečlivé ochraně. Je třeba vzít na vědomí, že ačkoliv by všechny osobní zdravotní informace měly být jednotně klasifikovány jako důvěrné, praktické ohledy mohou požadovat identifikaci záznamů subjektů péče, které tak mohou být vystaveny zvýšenému riziku zpřístupnění osobám, které nemají „potřebu něco znát“ (need to know). Takoví jednotlivci zahrnují zaměstnance samotné organizace (zvláště pokud jejich zdravotní stav vyvolává emotivní chování), šéfy vlád, celebrity, politiky, novináře a členy skupin čelících zvláště vysokým rizikům (například osoby s pohlavně přenosnými chorobami, nebo osoby, jejichž osobní zdravotní data obsahují informace o genetických předpokladech k vážným chorobám). Záznamy těchto jedinců je potřeba zvlášť označit, aby mohly být podrobně monitorovány. Těmto záměrům, jako je označováni citlivých informaci, musí být věnována zvláštní péče, aby se nestaly kontraproduktivními, tj. aby naopak neupoutaly pozornost na jednotlivé označené údaje. Je třeba zdůraznit, že ačkoliv jsou některé subjekty péče vystaveny zvýšenému riziku, jejich osobní zdravotní informace nejsou přirozeně více důvěrné, než informace jiných subjektů péče. Všechny osobní zdravotní informace jsou důvěrné a mělo by s nimi být nakládáno odpovídajícím způsobem.

Označování a zacházení s informacemi

Všechny zdravotnické informační systémy, zpracovávající osobní zdravotní informace, budou informovat uživatele o důvěrnosti osobních zdravotních informací dostupných ze systému (například při startu nebo přihlášení) a budou označovat jejich tištěné výstupy jako důvěrné, pokud obsahují osobní zdravotní informace.

Uživatelé systémů zdravotnických informací potřebují vědět, kdy data, ke kterým přistupují, obsahují osobní zdravotní informace. Za toto opatření ponese odpovědnost administrátor.

4.2.3 Bezpečnost z hlediska lidských zdrojů

Cílem bezpečnosti této oblasti je zajistit, aby zaměstnanci, smluvní a třetí strany byli srozuměni se svými povinnostmi, aby pro jednotlivé role byli vybráni vhodní kandidáti a snížit riziko lidské chyby, krádeže, podvodu nebo zneužití prostředků organizace.

Odpovědnosti za bezpečnost budou zohledněny v rámci přijímacího řízení, budou také zahrnuty v pracovních smlouvách a popisech práce. Potenciální uchazeči budou náležitě prověřeni, zejména v případě citlivých pracovních míst. Všichni zaměstnanci, smluvní a třetí strany, využívající zařízení organizace pro zpracování informací, podepíší dohodu odpovídající jejich rolím a povinnostem.

4.2.3.1 Před vznikem pracovního poměru

Role a odpovědnosti zaměstnanců, smluvních a třetích stran v oblasti bezpečnosti informací budou stanoveny a zdokumentovány v souladu s bezpečnostní politikou organizace.

Role a odpovědnosti v oblasti bezpečnosti informací budou zahrnovat:

a) požadavek na realizaci a dodržování zásad v souladu s bezpečnostní politikou organizace;
b) požadavek na ochranu aktiv před neautorizovaným přístupem, prozrazením, modifikací, zničením nebo narušením;
c) požadavek na vykonávání určitých bezpečnostních postupů nebo činností;
d) požadavek na určení jednoznačné odpovědnosti za provedené činnosti a možné postihy pokud dojde k porušení politiky bezpečnosti informací;
e) požadavek hlásit bezpečnostní události nebo jiná bezpečnostní rizika;
f) zajištění, že podmínky vztahující se k důvěrnosti osobních zdravotních informací přežijí ukončení pracovního poměru po neomezenou dobu (závazek zachování mlčenlivosti).

V rámci přijímacího řízení budou zájemcům o práci jasně sděleny role a odpovědnosti spojené s místem, o které se ucházejí. Za toto opatření bude odpovědný bezpečnostní manažer.

Všichni uchazeči o zaměstnání, smluvní a třetí strany budou prověřeni dle platných zákonů, předpisů a v souladu s etikou. Prověření budou prováděna na základě požadavků stanovených organizací, dále s ohledem na klasifikaci informací, ke kterým by měli získat přístup, ale také z hlediska jejich spolehlivosti a potenciálních rizik.

Při prověřování bude brán zřetel na dodržení soukromí a ochranu osobních dat a související legislativu. Zacházet se všemi dotyčnými dokumenty se bude v souladu se zákonem č. 101/2000 Sb., o ochraně osobních údajů, ve znění pozdějších předpisů.

Kromě dodržování těchto pokynů bude organizace ověřovat alespoň identitu, současné a předchozí zaměstnání již při podání žádosti o zaměstnání. Je důležité vědět, jak a kde lze kontaktovat odborný zdravotnický personál, protože někteří zaměstnanci pravidelně mění svá působiště a jejich podrobnosti o bydlišti mohou mít omezenou platnost. Zdravotnická organizace tudíž bude shromažďovat rozumný počet referencí a přijme i jiné formy ověřováni, například odbornými orgány a akademickými institucemi. Kontrola kriminální minulosti bude prováděna vždy.

Bezpečnostní manažer stanoví přesné postupy vymezující kritéria a omezení, např. kdo a jak je oprávněn prověrky provádět, kdy a jakým způsobem budou prověrky probíhat. Podobné prověrky budou prováděny také u externích pracovníků a pracovníků třetích stran.

V následující tabulce jsou uvedeny potřebné zdroje, odpovědnosti a harmonogramy spojený se zaváděním opatření:

Tabulka 4 Opatření 4.2.3.1

Položka	Přímý náklad (odhad)	Odpovědnost	Harmonogram nasazení opatření
Vypracování nových smluv	3000 Kč	Právní oddělení, bezp. manažer	Do 1 měsíce
Příprava úvodního školení	1000 Kč	Bezp. manažer	Do 1 měsíce
Prověrka uchazeče	0 Kč	Bezp. manažer	Při pohovoru
Celkem:	**4000 Kč**		

4.2.3.2 Během pracovního poměru

Cílem je zajistit, aby si zaměstnanci, smluvní a třetí strany byli vědomi bezpečnostních hrozeb a problémů s nimi spjatých, svých odpovědností a povinností a byli připraveni podílet se na dodržování politiky bezpečnosti informací během své běžné práce a na snižování rizika lidské chyby.

Budou jasně definovány odpovědnosti vedoucích zaměstnanců, aby se zajistilo dodržování bezpečnosti ze strany jednotlivců během celé doby trvání pracovního vztahu. Vedoucí zaměstnanci budou po uživatelích a smluvních a třetích stranách požadovat dodržování bezpečnosti v souladu se zavedenými politikami a směrnicemi. Zaměstnanci, smluvní a třetí strany budou školeni v bezpečnostních postupech a ve správném používání prostředků pro zpracování informací, aby byla minimalizována

bezpečnostní rizika. Budou vytvořena formalizovaná pravidla pro disciplinární řízení v případě narušení bezpečnosti.

Kromě dodržování těchto pokynů je důležité upozornit na zvláštní důraz, který je třeba věnovat obavám subjektů péče, které si nepřejí, aby k jejich osobním zdravotním informacím měli přístup ti zdravotníci, kteří jsou jejich sousedy, kolegy nebo příbuznými. Tyto obavy často tvoří velké procento stížností těch, kteří se obávají o důvěrnost svých osobních zdravotních informací. Stejně tak si zaměstnanci často nepřejí dostat se do pozice, kdy by měli přezkoumávat informace o svých známých, příbuzných či sousedech.

V následující tabulce jsou uvedeny potřebné zdroje, odpovědnosti a harmonogramy spojené se zaváděním opatření:

Tabulka 5 Opatření 4.2.3.2

Položka	Přímý náklad (odhad)	Odpovědnost	Harmonogram nasazení opatření
Příprava pravidelného školení	**3000 Kč**	Bezp. manažer	Do 1 měsíce, 1x-2x do roka

4.2.3.3 Ukončení nebo změna pracovního poměru

Cílem je zajistit, aby ukončení nebo změna pracovního vztahu zaměstnanců a smluvních a třetích stran proběhla řádným způsobem.

Budou určeny jednoznačné odpovědnosti za řádný průběh ukončení pracovního vztahu zaměstnanců, smluvních a třetích stran, za odevzdání přiděleného vybavení a odejmutí přístupových práv. Při ukončení pracovního vztahu odevzdají zaměstnanci, pracovníci smluvních a třetích stran veškeré jim svěřené předměty, které jsou majetkem organizace.

Změna odpovědností a pracovního vztahu v rámci organizace by měla probíhat jako by se jednalo o odebrání odpovědností nebo ukončení pracovního vztahu.

Kromě těchto pokynů je důležité si uvědomit, že ve zdravotnictví mnohé z pracovních pozic, například lékaři a sestry všeobecně procházejí výukovými programy a jinými „rotacemi“, kde se jejich přístupová práva mohou zásadně změnit. Pro zajištění ukončení předchozích práv, která pro svou další roli již nepotřebují, je potřeba takové změny provádět stejným způsobem jako při ukončováni pracovního poměru.

Odebráni přístupových práv

Organizace musí co možná nejdříve ukončit přístupová privilegia vztahující se k osobním zdravotním informacím všem odcházejícím nebo dočasným zaměstnancům, smluvním třetím stranám a dobrovolníkům ihned po ukončení zaměstnání, smlouvy nebo dobrovolných aktivit. Organizace by měla zvážit okamžité odebrání přístupových práv po oznámení odstoupení, výpovědi atd., kdykoliv hrozí zvýšené riziko plynoucí z trvání takového přístupu.

Celý proces ukončení pracovního vztahu bude formalizovaný a bude zahrnovat navrácení poskytnutého programového vybavení, dokumentů a vybavení, které jsou majetkem organizace. Nesmí se opomenout také další předměty, jako například mobilní výpočetní prostředky, kreditní karty, přístupové karty, programová dokumentace a informace uložené na elektronických mediích.

Bude zajištěno zálohování a bezpečné smazání informací uložených na zařízení, které bylo odkoupeno nebo je majetkem zaměstnance, smluvní nebo třetí strany.

V nově vypracovaných smlouvách musí být dodatek o celoživotní mlčenlivosti ohledně práce s osobními zdravotními informacemi. Toto se zahrne už do opatření 4.2.3.1, ale platí i po ukončení pracovního poměru.

V následující tabulce jsou uvedeny potřebné zdroje, odpovědnosti a harmonogramy spojené se zaváděním opatření:

Tabulka 6 Opatření 4.2.3.3

Položka	Přímý náklad (odhad)	Odpovědnost	Harmonogram nasazení opatření
Odevzdání majetku organizace	0 Kč	Přímý nadřízený	Ihned
Odejmutí práv k přístupu do IS	0 Kč	Administrátor	Ihned
Zálohy a smazání dat na odkoupeném zařízení	500 Kč	Administrátor	Ihned
Vypracování nových smluv	3000 Kč	Právní oddělení, bezp. manažer	Do 1 měsíce
Celkem:	**3500 Kč**		

4.2.4 Fyzická bezpečnost a bezpečnost prostředí

Cílem je předcházet neautorizovanému přístupu do vymezených prostor, předcházet poškození a zásahům do provozních budov a informací organizace. Předcházet ztrátě, poškození nebo kompromitaci aktiv a přerušení činnosti organizace.

Zařízení zpracovávající kritické nebo citlivé informace organizace, budou umístěny v zabezpečených zónách chráněných definovaným bezpečnostním perimetrem s odpovídajícími bezpečnostními bariérami a vstupními kontrolami. Tato zařízení budou fyzicky chráněna proti neautorizovanému přístupu, poškození a narušení. Zařízení budou fyzicky chráněna proti bezpečnostním hrozbám a působení vnějších vlivů.

Pozornost bude věnována také jejich umístění a likvidaci. Na ochranu proti možnému ohrožení nebo neautorizovanému přístupu a na ochranu podpůrných prostředků, jako například dodávky elektrické energie a struktury kabelových rozvodů, budou požadována zvláštní opatření.

4.2.4.1 Bezpečné oblasti

Při ochraně prostor, ve kterých se nachází zdravotní osobní informace nebo zařízení pro zpracování těchto informací budou používány bezpečnostní perimetry (bariéry jako například zdi, vstupní turniket na karty nebo recepce).

Následující doporučení a opatření budou podle vhodnosti implementována:

a) Bude jasně definován bezpečnostní perimetr, umístění a úroveň každého bezpečnostního perimetru bude záviset na bezpečnostních požadavcích na aktiva, uvnitř perimetru, a na výsledku hodnocení rizik;
b) perimetr budovy nebo oblasti obsahující zařízení pro zpracování informací bude v řádném stavu (tj. nebudou v perimetru nebo v oblasti existovat slabá, lehce proniknutelná místa). Obvodové zdi objektu budou mít pevnou konstrukci a vstupní dveře budou chráněny před neautorizovaným vstupem, zabezpečeny kontrolními mechanizmy např. mřížemi, alarmy, zámky apod. Dveře a okna musí být v případě nepřítomnosti uzavřeny. U oken, zejména pokud jsou v přízemí, bude zváženo využití externích ochranných prvků;
c) fyzické bariéry budou, tam kde je to použitelné, postaveny tak, aby chránily před neoprávněným vstupem a kontaminací;

d) požární dveře v bezpečnostním perimetru budou opatřeny elektronickým zabezpečovacím systémem (EZS) a budou monitorovány. Požární dveře (stejně tak i zdi) budou splňovat požadovanou úroveň odolnosti, dle příslušných požadavků místních, národních a mezinárodních norem;
e) zařízení pro zpracování informací spravované organizací budou fyzicky oddělena od prostředků třetích stran.

Zabezpečenou oblastí může být uzamykatelná kancelář nebo několik místností uvnitř fyzického bezpečnostního perimetru. Bude aplikováno fyzické zabezpečení kanceláří, místností a zařízení. Aby bylo zajištěno, že je přístup do zabezpečených oblastí povolen pouze oprávněným osobám, měly by být tyto oblasti chráněny vhodným systémem kontrol vstupu. Na ochranu proti škodám způsobeným požárem, povodní, zemětřesením, výbuchem, civilními nepokoji a jinými přírodními nebo lidmi zapříčiněnými katastrofami budou aplikovány prvky fyzické ochrany. Bude zajištěno a vhodně umístěno hasicí zařízení. Záložní zařízení a zálohovací média budou umístěna v takové bezpečné vzdálenosti, aby se zabránilo jejich případnému zničení v případě havárie v hlavních prostorách.

V následující tabulce jsou uvedeny potřebné zdroje, odpovědnosti a harmonogramy spojené se zaváděním opatření:

Tabulka 7 Opatření 4.2.4.1

Položka	Přímý náklad (odhad)	Odpovědnost	Harmonogram nasazení opatření
Definování bezpečnostního perimetru	1500 Kč	Bezpečnostní manažer, hlavní projektant	Do 14 dnů
Zabezpečení perimetru	20000 Kč – 40000 Kč	Bezpečnostní manažer	Do 1 měsíce
Kontrola řádného stavu	1000 Kč	Bezpečnostní manažer, auditor	Ihned po rekonstrukci, 1x za 3-6 měsíců
Celkem:	**až 42500 Kč**		

Kromě těchto pokynů je důležité vzít na vědomí, že v mnoha zdravotnických zařízeních je konkretizace bezpečnostních perimetrů zvláště náročná. Subjekty péče pronikly do mnoha provozních oblastí. Pravděpodobně neexistuje žádné jiné průmyslové odvětví, kde má veřejnost tak rozšířený přístup do provozních oblastí, jako je zdravotnictví. Zároveň je potřeba udržovat bezpečné prostředí pro fyzické

zabezpečení subjektů péče, stejně jako zabezpečení dat a systémů, ke kterým může být v tomto prostředí přístup.

Klienti ve zdravotnictví, na rozdíl jiných průmyslových sektorů, často nejsou schopni zajistit svou vlastní osobní bezpečnost. Míra fyzické bezpečnosti informací by měla být koordinována s fyzickou bezpečností a s mírou fyzické bezpečnosti pro subjekty péče. Zdravotnické organizace mají povinnost chránit obojí.

4.2.4.2 Bezpečnost zařízení

Zařízení budou umístěna a chráněna tak, aby se snížila rizika hrozeb a nebezpečí daná prostředím a aby se omezily příležitosti pro neoprávněný přístup.

Budou zváženy následující opatření:

a) kde je to možné, zařízení budou umístěna tak, aby byl minimalizován nadbytečný přístup do pracovních prostor;
b) zařízení pro zpracování a ukládání citlivých dat budou umístěna tak, aby bylo sníženo riziko možného odezírání informací;
c) aktiva, která vyžadují zvláštní ochranu, budou izolována, aby se snížil rozsah požadované celkové ochrany;
d) pro minimalizaci rizik potenciálních hrozeb (např. krádež, oheň, výbušniny, kouř, voda, vibrace, prach, působení chemických látek, rušení elektrického napájení, elektromagnetické vyzařování a vandalismus) budou přijata odpovídající opatření;
e) organizace zváží svá pravidla týkající se jídla, pití a kouření v blízkosti zařízení zpracovávajících informace;
f) působení vnějšího prostředí (jako např. teplota a vlhkost), které by mohlo mít vliv na činnost zařízení pro zpracování informací, bude monitorováno;
g) ve všech budovách bude nasazena ochrana proti blesku a ochrannými filtry proti blesku budou osazeny všechny vnější komunikační linky a elektrické vedení;
h) zařízení zpracovávající citlivé informace bude chráněno, aby se zabránilo úniku citlivých informací prostřednictvím kompromitujícího (parazitního) elektromagnetického vyzařování.

Zařízení budou chráněna před selháním napájení a před dalšími výpadky způsobenými selháním podpůrných služeb. Pro elektrická zařízení zajišťující kritické operace organizace bude použito záložních zdrojů UPS, umožňující korektní ukončení

nebo pokračování v práci. Do plánů obnovy funkčnosti budou zapracovány činnosti prováděné v případě selhání UPS. UPS bude pravidelně kontrolována, zda má odpovídající kapacitu a testována v souladu s doporučeními výrobce. Při nutnosti zpracovávání informací v případě déletrvajících výpadků proudu bude zavedeno použití záložního generátoru. UPS a generátor budou pravidelně kontrolovány, aby se zajistilo, že mají dostatečnou kapacitu a budou také pravidelně testovány podle návodu výrobce. V místnostech se zařízením v blízkosti nouzových východů budou instalovány bezpečnostní (nouzové) vypínače pro rychlé vypnutí napájení v případě nebezpečí. Pro případ výpadku hlavního napájení bude zajištěno nouzové osvětlení. Dodávky vody budou stabilní a dostatečné pro zajištění klimatizace a pro automatické hasící systémy (pokud jsou používány). Selhání dodávek vody může zapříčinit poškození lékařských zařízení. Telekomunikační zařízení bude k poskytovateli služby připojeno nejméně dvěma různými cestami, aby se zabránilo selhání hlasových služeb v případě, že dojde k výpadku na jedné z cest. Hlasové služby budou odpovídat legislativním požadavkům krizové komunikace. Mezi možnosti jak dosáhnout kontinuity napájení patří znásobení přívodů dodávek energie, aby zařízení nebylo závislé na jednom zdroji.

Silové a telekomunikační kabelové rozvody, které jsou určeny pro přenos dat a podporu informačních služeb, budou chráněny před poškozením či odposlechem.

Pro bezpečnost kabelových rozvodů budou zvážena následující doporučení:

a) napájecí a telekomunikační linky připojené k prostředkům IT budou tam, kde je to možné, vést pod zemí nebo budou chráněny jiným vhodným způsobem;
b) síťové kabelové rozvody budou chráněny před neoprávněným odposlechem nebo poškozením, například vedením v kolektoru anebo tím, že nebudou vedeny přes veřejné prostory;
c) napájecí kabely budou odděleny od komunikačních rozvodů, aby se zabránilo interferenci;
d) kabely a zařízení budou zřetelně označeny tzv. identifikátory, aby se zabránilo možnosti záměny v případech provádění oprav poškozených kabelů nebo při zpětném zapojení kabelů po výkonu práce uklízečky;
e) pro snížení pravděpodobnosti vzniku chyb bude udržován seznam propojení;

Navíc ještě bude zváženo použití optických kabelů, kde je to možné, nebo alespoň stínění kabeláže proti rušení interferencí.

Všechna jak lékařská zařízení tak i zařízení zpracovávající zdravotní osobní data budou správně udržována pro zajištění jejich stálé dostupnosti a integrity.

Lékařská zařízení, která zaznamenávají či poskytují údaje, mohou také vyžadovat speciální bezpečnostní úvahy vzhledem k prostředí, ve kterém jsou provozována a vzhledem k výskytu magnetického záření, které při jejich provozu vzniká. Zdravotnické organizace, zvláště nemocnice by měly svými směrnicemi o umístění a ochraně IT zařízení zajistit minimální vystavení takovému záření.

Použití zařízení pro zpracování informací, bez ohledu na jejich vlastníka, mimo budovy pobočky organizace by mělo podléhat schválení vedením organizace.

Při práci mimo prostory organizace budou zvážena následující doporučení:

a) při cestách mimo organizaci nebudou zařízení a média ve veřejných prostorách ponechána bez dozoru. Přenosný počítač bude přepravován jako příruční zavazadlo a v rámci možností ukrýván;
b) budou se dodržovat pokyny výrobce týkající se ochrany zařízení, například zajištění ochrany proti působení silného magnetického pole;
c) pro práci doma budou určena vhodná opatření na základě hodnocení rizik, například uzamykatelné skříňky, pravidlo prázdného stolu, kontrola přístupu k počítači a zabezpečení spojení s kanceláří;
d) zařízení používané mimo prostory organizace budou pojištěna.

Bezpečnostní rizika, jako například poškození, krádež a odposlech, se mohou v různých lokalitách značně lišit a to by mělo být zváženo při výběru těch nejvhodnějších bezpečnostních opatření.

Zařízení pro zpracování informací zahrnují všechny druhy osobních počítačů, organizérů, mobilních telefonů, čipových karet, dokumentů a ostatních zařízení, používaných pro práci doma nebo vynášených mimo normální pracovní umístění.

Kromě dodržování těchto pokynů musí organizace zpracovávající osobní zdravotní informace zajistit, aby jakékoliv použití lékařských zařízení, zaznamenávajících a poskytujících data mimo budovy bylo autorizováno. To by se mělo týkat i zařízení, která používají pracovníci v terénu (tj. pokud představují hlavní charakteristiku role zaměstnance, jako je personál v sanitce, terapeuti apod.).

Všechna zařízení obsahující paměťová média budou kontrolována tak, aby bylo možné zajistit, že před jejich likvidací nebo opakovaným použitím budou citlivá data a

licencované programové vybavení nevratně odstraněna nebo přepsána. U zařízení obsahujících zdravotní osobní informace bude preferováno fyzické zničení nebo bezpečné smazání/přepsání dat za použití postupů znemožňujících jejich obnovu.

Zařízení, informace nebo programové vybavení nebude bez schválení přemisťováno.

V následující tabulce jsou uvedeny potřebné zdroje, odpovědnosti a harmonogramy spojené se zaváděním opatření:

Tabulka 8 Opatření 4.2.4.2

Položka	Přímý náklad (odhad)	Odpovědnost	Harmonogram nasazení opatření
Správné umístění zařízení	0 Kč	Bezp. manažer, vlastníci aktiv	Ihned po rekonstrukci
Vytvoření směrnic o podmínkách použití zařízení	5000 Kč	Bezpečnostní manažer, administrátor	Do 2 měsíců
Kontrola umístění zařízení	500 Kč	Bezpečnostní manažer, auditor	Ihned, 1x za 6 měsíců
Nasazení ochran proti blesku	2000 Kč	Bezp. manažer	Ihned
Nasazení záložních zdrojů	7000 Kč	Bezp. manažer	Ihned
Kontrola dodávek vody	0 Kč	Vedoucí pracoviště	Ihned, 1x do měsíce
Bezpečnost kabelových rozvodů	15000 Kč – 30000 Kč	Bezp. manažer, správce sítě	Do 1 měsíce
Vytvoření seznamu propojení	500 Kč	Správce sítě	Ihned při zapojování
Pojištění zařízení	20000 Kč	Bezp. manažer	Do 2 měsíců
Bezpečné smazání nepotřebných dat	500 Kč	Administrátor	Ihned
Celkem:	**až 65500 Kč**		

4.2.5 Řízení komunikací a řízení provozu

Cílem řízení komunikací a provozu je zajistit správný a bezpečný provoz prostředků pro zpracování informací.

4.2.5.1 Provozní postupy a odpovědnosti

Budou stanoveny odpovědnosti a postupy pro řízení a správu prostředků zpracovávajících informace. Zahrnuje to vytváření vhodných provozních instrukcí a postupů.

Provozní postupy, jako jsou například spuštění a zastavení systému, zálohování dat, údržba zařízení, zacházení s médii, správa počítačové místnosti, zacházení s korespondencí a bezpečnost práce, budou zdokumentovány a udržovány a budou dostupné všem uživatelům dle potřeby.

Změny ve vybavení a zařízení pro zpracování informací budou řízeny a budou uchovávány veškeré relevantní informace, například v podobě auditních záznamů. Změny provozních systémů by měly být prováděny pouze v nutných případech, například dojde-li k nárůstu rizika. Instalace nejnovějších verzí provozních systémů a aplikací by měla být předem dobře zvážena. Může zavést nové zranitelnosti a způsobit větší nestabilitu systému než předchozí verze, často je také spojena s dodatečným zaškolením personálu, s licenčními poplatky, poplatky za podporu a údržbu, nákupem nového hardwaru a dodatečnou administrací.

V následující tabulce jsou uvedeny potřebné zdroje, odpovědnosti a harmonogramy spojené se zaváděním opatření:

Tabulka 9 Opatření 4.2.5.1

Položka	Přímý náklad (odhad)	Odpovědnost	Harmonogram nasazení opatření
Vytvoření směrnic a provozních postupů	4000 Kč	Vedoucí pracovník, administrátor, bezp. manažer	Do 1 měsíce
Vytvoření seznamu konkrétních aktiv	2500 Kč	Administrátor, bezp. manažer	Do 1 měsíce
Kontrola dodržování směrnic	2000 Kč	Auditor ISMS	Ihned, 1x za 6 měsíců
Celkem:	**8500 Kč**		

4.2.5.2 Řízení dodávek služeb třetích stran

Cílem je zavést a udržovat přiměřenou úroveň bezpečnosti informací a úroveň dodávky služeb ve shodě s uzavřenými dohodami.

Pro zajištění toho, že služby dodávané třetími stranami jsou v souladu s dohodnutými požadavky, bude organizace kontrolovat realizaci dohod, monitorovat míru souladu jejich dodržování a v případě potřeby zajišťovat nápravu. Služby, zprávy a záznamy poskytované třetí stranou budou monitorovány a pravidelně přezkoumávány, audity budou opakovány v pravidelných intervalech. Tato opatření se týkají celé organizace, což je nad rámec této práce. V následující tabulce jsou uvedeny potřebné zdroje, odpovědnosti a harmonogramy spojené se zaváděním opatření:

Tabulka 10 Opatření 4.2.5.2

Položka	Přímý náklad (odhad)	Odpovědnost	Harmonogram nasazení opatření
Vytvoření a přezkoumání smluv se třetími stranami	4000 Kč	Právní oddělení, bezp. manažer	Do 3 měsíců
Kontrola a monitoring zpráv třetích stran	2000 Kč	Auditor	Ihned, 1x za 3 měsíce
Celkem:	**6000 Kč**		

4.2.5.3 Plánování a akceptace systémů

Cílem je minimalizovat riziko selhání informačních systémů.

Pro zajištění odpovídající kapacity a zdrojů a výkonu informačního systému je nutné provést odpovídající přípravu a plánování. Aby se snížilo riziko přetížení systému, bude vytvářen odhad budoucích kapacitních požadavků. Před schválením nových systémů a před jejich uvedením do provozu k nim budou stanoveny, písemně zdokumentovány a otestovány provozní požadavky.

Pro zajištění požadovaného výkonu informačního systému, s ohledem na budoucí kapacitní požadavky, bude monitorováno, nastaveno a projektováno využití zdrojů. Budou určena kritéria pro přejímání nových informačních systémů, jejich aktualizaci a zavádění nových verzí a vhodný způsob testování systému v průběhu vývoje a před zavedením do ostrého provozu. Kromě dodržování těchto pokynů musí organizace stanovit akceptační kritéria pro plánované nové informační systémy, upgrady a nové verze. Před jejich schválením musí organizace vhodným způsobem systém otestovat.

V následující tabulce jsou uvedeny potřebné zdroje, odpovědnosti a harmonogramy spojené se zaváděním opatření:

Tabulka 11 Opatření 4.2.5.3

Položka	Přímý náklad (odhad)	Odpovědnost	Harmonogram nasazení opatření
Odhad kapacitních požadavků	1000 Kč	Administrátor, správce sítě	Ihned
Monitorování využití zdrojů	500 Kč	Administrátor, správce sítě	Ihned, 1x za 3 měsíce
Stanovení akceptačních kritérií nových verzí IS	1500 Kč	Bezp. manažer	Do 3 měsíců
Celkem:	**3000 Kč**		

4.2.5.4 Ochrana proti škodlivým a mobilním programům (kódům)

Cílem je chránit integritu programů a dat. Pro prevenci a detekování škodlivých programů a nepovolených mobilních kódů jsou vyžadována patřičná opatření. Programy a zařízení pro zpracování informací jsou zranitelné škodlivými programy, jako jsou například počítačové viry, síťoví červi, trojští koně a logické bomby. Uživatelé budou upozorňováni na nebezpečí neschválených a škodlivých programů. Vedoucí zaměstnanci budou tam, kde je to vhodné, aplikovat zvláštní opatření pro jejich předcházení a detekování a zavádět postupy odstranění škodlivých programů a kontroly mobilních kódů.

Ochrana proti škodlivým programům bude založena na detekci škodlivých programů, opravných programů, na bezpečnostním povědomí, dále na vhodném přístupu k systému a na opatřeních zajišťujících řízení změn.

Budou implementována následující opatření:

a) ustavení formálních pravidel požadujících dodržování licenčních podmínek a zákaz používání neschváleného programového vybavení;
b) ustavení formálních pravidel zajišťujících ochranu proti rizikům vyplývajícím ze získávání programů z externích sítí nebo z jiných médií a určujících, jaká ochranná opatření budou přijata;
c) instalace a pravidelná aktualizace antivirových detekčních a opravných programů pro kontrolu počítačů a médií, buď jako preventivní prostředek využívaný ad-hoc způsobem, nebo pravidelně. Prováděné kontroly budou zahrnovat:

a. ověření všech souborů na elektronických nebo optických médiích nejistého a neověřeného původu nebo souborů získaných prostřednictvím neautorizovaných sítí před jejich použitím na přítomnost škodlivých programů;
b. testování všech příloh elektronické pošty a stažených dat na přítomnost škodlivých programů před jejich použitím. Tato kontrola může být prováděna na různých místech, například na poštovním serveru, na pracovních stanicích nebo při vstupu do sítě organizace;
c. kontrola obsahu webových stránek na přítomnost škodlivého kódu;

d) zavedení pravidelného sběru nových informací (odběr časopisů, hledání na internetu) o nových škodlivých kódech;

Pro zajištění odpovídající ochrany lze antivirové programy nastavit tak, aby automaticky probíhala aktualizace definičních souborů a skenovacího enginu. Antivirové programy budou nainstalovány na každé pracovní stanici.

Použití povolených mobilních kódů bude nastaveno v souladu s bezpečnostní politikou, bude zabráněno spuštění nepovolených mobilních kódů. Mobilní kód je programový kód, který se přenáší z jednoho počítače na druhý a poté se automaticky spustí a vykoná specifickou funkci za minimální nebo žádné součinnosti s uživatelem. Mobilní kódy jsou součástí řady middleware služeb (např. zajišťujících propojení jednotlivých aplikací).

V následující tabulce jsou uvedeny potřebné zdroje, odpovědnosti a harmonogramy spojené se zaváděním opatření:

Tabulka 12 Opatření 4.2.5.4

Položka	Přímý náklad (odhad)	Odpovědnost	Harmonogram nasazení opatření
Nastavení politiky firewallů	500 Kč	Správce sítě	Ihned
Nastavení aktualizací antivirů, operačních systémů a použitých programů	500 Kč	Administrátor	Ihned
Celkem:	**1000 Kč**		

4.2.5.5 Zálohování zdravotnických informací

Cílem je udržovat integritu a dostupnost informací a zařízení pro jejich zpracování. Budou vytvořeny rutinní postupy realizující schválenou politiku zálohování a strategii pro vytváření záložních kopií dat a testování jejich včasného obnovení. Záložní kopie důležitých informací a programového vybavení organizace budou pořizovány a testovány v pravidelných intervalech.

Budou implementovány následující opatření:

a) bude stanoveno minimální nutné množství vytvářených záloh;
b) budou vytvořeny přesné a úplné záznamy o záložních kopiích s popsanými postupy obnovy;
c) rozsah vytvářených záloh (např. kompletní nebo přírůstkové zálohy) a frekvence s jakou jsou vytvářeny, bude odpovídat požadavkům organizace na dostupnost informací, požadavkům na bezpečnost informací a jejich kritičnosti z hlediska kontinuity činností organizace;
d) zálohy budou uloženy na bezpečném místě, v dostatečné vzdálenosti od sídla organizace, aby v případě havárie nebyly poškozeny nebo zničeny;
e) záložním informacím bude věnována přiměřená úroveň fyzické a vnější ochrany, odpovídající normám v hlavním sídle. Opatření používaná pro média v hlavním sídle bude rozšířena i na místo s uloženými záložními kopiemi;
f) záložní média budou pravidelně testována, aby bylo zajištěno, že se na ně lze v nutném případě spolehnout;
g) obnovovací postupy budou pravidelně prověřovány a testovány, aby se potvrdilo, že jsou účinné a že mohou být provedeny v čase vymezeném provozním obnovovacím postupům;
h) v případech, kdy je požadováno zajištění důvěrnosti zálohovaných informací, bude použito šifrování.

V následující tabulce jsou uvedeny potřebné zdroje, odpovědnosti a harmonogramy spojené se zaváděním opatření:

Tabulka 13 Opatření 4.2.5.5

Položka	Přímý náklad (odhad)	Odpovědnost	Harmonogram nasazení opatření
Vytvoření záznamů o záložních kopiích s popsanými postupy obnovy	2500 Kč	Bezp. manažer, koordinátor řízení kontinuity činností	Do 14 dnů
Testování záložních médií a obnovovacích postupů	3000 Kč	Bezp. manažer, koordinátor řízení kontinuity činností	Ihned, 1x za 6 měsíců
Celkem:	**5500 Kč**		

4.2.5.6 Správa bezpečnosti sítě

Komunikační trasy v ČR patří do tzv. kritické informační infrastruktury, jejíž zabezpečení řeší již zmiňovaný zákon o kybernetické bezpečnosti. Podle tohoto zákona musí provozovatel této části kritické infrastruktury vytvořit zvláštní štáb na ochranu poskytovaných služeb a na hlášení o bezpečnostních incidentech.

Cílem je zajistit ochranu informací v počítačových sítích a ochranu jejich infrastruktury. Pozornost vyžaduje správa bezpečnosti počítačových sítí, které mohou přesahovat hranice organizace. Pro zabezpečení citlivých dat přenášených veřejnými sítěmi jsou požadována dodatečná opatření. Pro zajištění ochrany před možnými hrozbami, pro zaručení bezpečnosti systémů a aplikací využívajících sítí a pro zajištění bezpečnosti informací při přenosu by počítačové sítě měly být vhodným způsobem spravovány a kontrolovány. Odpovědnost za provoz sítě bude oddělena od odpovědnosti za provoz počítačů. Budou stanoveny odpovědnosti a postupy pro správu vzdálených zařízení, včetně zařízení v prostorách uživatelů. Budou zavedena zvláštní opatření, která budou zajišťovat důvěrnost a integritu dat přenášených veřejnými nebo bezdrátovými sítěmi a ochranu připojených systémů a aplikací. Pro zajištění dostupnosti síťových služeb a připojených počítačů jsou vyžadována zvláštní opatření. Budou zavedeny vhodné postupy zaznamenávání a monitorování událostí souvisejících s bezpečností. Budou identifikovány a do dohod o poskytování síťových služeb zahrnuty bezpečnostní prvky, úroveň poskytovaných služeb a požadavky na správu všech síťových služeb a to jak v případech, kdy jsou tyto služby zajišťovány interně, tak

i v případech, kdy jsou zajišťovány cestou outsourcingu. Budou identifikována bezpečnostní nastavení spojená s konkrétními službami, jako jsou bezpečnostní prvky, úroveň poskytovaných služeb a požadavky na jejich správu. Organizace se bude snažit zajistit implementaci těchto opatření poskytovatelem síťových služeb. Síťové služby zahrnují poskytnutí připojení, služby privátních sítí, sítí s přidanou hodnotou a správu bezpečnostních řešení jako jsou například bezpečnostní brány (firewall) a systémy pro detekci průniku. Bezpečnostní prvky síťových služeb zahrnují technologie použité pro zajištění bezpečnosti síťových služeb, jako např. autentizace, šifrování a kontroly síťových spojení, a také postupy omezující přístup k síťovým službám nebo k aplikacím. V následující tabulce jsou uvedeny potřebné zdroje, odpovědnosti a harmonogramy spojené se zaváděním opatření:

Tabulka 14 Opatření 4.2.5.6

Položka	Přímý náklad (odhad)	Odpovědnost	Harmonogram nasazení opatření
Vytvoření směrnic pro práci v síti	5000 Kč	Správce sítě, bezp. manažer	Do 1 měsíce
Kontrola a monitorování provozu na síti	1000 Kč	Správce sítě, bezp. manažer	Ihned, 1x za 14 dní
Kontrola zabezpečení sítě	1000 Kč	Správce sítě, auditor ISMS	Ihned, 1x za 1 měsíc
Celkem:	**7000 Kč**		

4.2.5.7 Zacházení s médii

Cílem je předcházet neoprávněnému prozrazení, modifikaci, ztrátě nebo poškození aktiv a přerušení činnosti organizace. Média budou kontrolována a fyzicky zabezpečena. Budou stanoveny náležité provozní postupy týkající se zabezpečení dokumentů, počítačových médií (např. pásky, disky), vstupních/výstupních dat a systémové dokumentace před neoprávněným prozrazením, modifikací, odstraněním nebo poškozením.

Budou implementována následující opatření:

a) pokud již nejsou znovupoužitelná média potřebná, bude předtím, než jsou odstraněna z organizace, vymazán jejich obsah;
b) v nutných případech bude požadována autorizace pro odstranění médií z organizace a bude se o tom vést záznam pro potřeby auditu;

c) ukládat všechna média v bezpečném prostředí v souladu se specifikacemi výrobce;
d) informace, u kterých požadavek na dostupnost přesahuje životnost médií (dle specifikací výrobce) na kterých jsou uloženy, budou přemístěny, aby se zabránilo jejich případné ztrátě;
e) zaregistrování všech vyměnitelných médií pro snížení pravděpodobnosti jejich ztráty;
f) použití vyměnitelných mechanik bude povoleno jen v odůvodněných případech.

Kromě dodržování těchto pokynů bude organizace zajišťovat, že veškeré osobní zdravotní informace uložené na výměnných médiích jsou zašifrované po dobu jejich přepravy, nebo chráněné před krádeží, když jsou média přepravována. Vyměnitelná média zahrnují pásky, disky, flashdisky, přenositelné harddisky, CD, DVD a tiskové výstupy.

Jestliže jsou média dále provozně neupotřebitelná, budou bezpečně a spolehlivě zlikvidována. Při nedbalé likvidaci médií by se mohla citlivá data dostat do cizích rukou. Pro minimalizaci tohoto rizika budou vytvořeny formální postupy bezpečné likvidace médií. Postupy pro bezpečnou likvidaci budou odpovídat citlivosti informací.

Budou implementována následující opatření:

a) média, obsahující citlivé informace, budou bezpečně zlikvidována, například spálením nebo skartováním nebo smazáním dat před jejich opětovným použitím jiným způsobem v rámci organizace;
b) budou vytvořeny postupy pro identifikaci médií, které vyžadují bezpečnou likvidaci;
c) může být jednodušší stanovit pravidla bezpečného sběru a likvidace pro všechna média, než se snažit vyčlenit ta s citlivými daty;
d) řada organizací nabízí sběr a likvidaci papíru, zařízení a médií. Při výběru vhodného smluvního partnera je nutné dávat zejména pozor na to, aby dodržoval odpovídající opatření a měl zkušenosti;
e) likvidace citlivých médií by měla být, podle možností, zaznamenávána pro potřeby následného auditu.

Nedostatečná likvidace nosičů dat je nadále zdrojem vážných narušení důvěrnosti informací o pacientech. Je zvláště důležité si uvědomit, že by tato opatření měla být

zavedena před tím, než dojde k opravě nebo likvidaci jakéhokoliv propojeného zařízení. Tento požadavek se vztahuje také na lékařská zařízení, která zaznamenávají či poskytují data. Pro zabránění neautorizovanému přístupu nebo zneužití informací by měla být stanovena pravidla pro manipulaci s nimi a pro jejich ukládání. Kromě těchto pokynů musí média obsahující osobni zdravotní informace být buďto chráněna fyzicky nebo musí být data, která obsahují bezpečně zašifrována.

V následující tabulce jsou uvedeny potřebné zdroje, odpovědnosti a harmonogramy spojené se zaváděním opatření:

Tabulka 15 Opatření 4.2.5.7

Položka	Přímý náklad (odhad)	Odpovědnost	Harmonogram nasazení opatření
Kontrola zabezpečení médií	1500 Kč	Administrátor, bezp. manažer	Ihned, 1x za 6 měsíců
Vytvoření směrnic o zacházení s médii	2500 Kč	Administrátor, bezp. manažer	Do 2 měsíců
Registrace všech vyměnitelných médií	500 Kč	Administrátor	Ihned
Vytvoření směrnic o likvidaci médií	2000 Kč	Administrátor, bezp. manažer	Do 1 měsíce
Celkem:	**6500 Kč**		

4.2.5.8 Výměna informací

Cílem je zajistit bezpečnost informací a programů při jejich výměně v rámci organizace a při jejich výměně s externími subjekty. Výměna informací a programů mezi organizacemi bude založena na formální politice, prováděna v souladu s platnými dohodami a bude ve shodě s platnou legislativou. Budou stanoveny postupy a směrnice pro ochranu informací a jejich nosičů při přepravě pro všechny typy používaných komunikačních zařízení. Bude zváženo následující:

a) postupy určené na ochranu informací před jejich zachycením, odposlouchávánim, zkopírováním, modifikací, špatným směrováním a zničením;
b) postupy detekce a ochrany před škodlivými kódy, které mohou být přenášeny elektronickou poštou;
c) postupy na ochranu citlivých informací přenášených v přílohách elektronické pošty;

d) politika a směrnice upravující použití zařízení pro elektronickou komunikaci;
e) odpovědnost zaměstnanců, smluvních a třetích stran za to, že nezkompromitují organizaci, například odesláním hanlivých zpráv, použitím elektronické pošty k obtěžování či neautorizovaným nákupům, atd.;
f) použití kryptografických technik pro zajištění důvěrnosti, integrity a autentičnosti přenášených informací;
g) vytvoření pravidel pro uchování a likvidace veškeré obchodní korespondence, včetně elektronické pošty v souladu s místní legislativou a předpisy;
h) zavedení opatření a omezení souvisejících s přesměrováním elektronické komunikace, např. automatické přeposílání elektronické pošty na externí emailovou adresu;
i) připomínání zaměstnancům, že mají dodržovat adekvátní opatrnost, například neprobírat citlivé informace, které by mohly být při telefonování zaslechnuty či odposlechnuty:
    a. osobami v bezprostřední blízkosti, zejména při použití mobilního telefonu;
    b. instalovaným odposlechem nebo jinou formou elektronického odposlouchávání umožněného fyzickým přístupem k telefonnímu přístroji nebo telefonní lince nebo použitím prohledávacích přijímačů při použití analogových mobilních nebo bezdrátových telefonů;
    c. dalšími osobami na druhé straně telefonu;
j) nenechávat zprávy na záznamníku, protože tyto zprávy mohou být přehrány neautorizovanou osobou, uloženy do veřejné sítě nebo uloženy jako výsledek chybného telefonátu;
k) upozorňování zaměstnanců na problémy spojené s použitím faxů, zejména:
    a. neautorizovaný přístup k vnitřním pamětem pro uchování faxových zpráv
    b. úmyslné přeprogramování faxu tak, aby posílal zprávy na specifická čísla;
    c. posílání dokumentů a zpráv na špatné místo z důvodu překlepu v čísle;
l) upozorňování zaměstnanců na to, že moderní faxová zařízení a kopírky používají vyrovnávací paměť, ve které je uložen obsah tištěných stránek, pro případ, že v zásobníku dojde papír nebo nastane chyba při přenosu dat.

Zaměstnanci budou dále upozorněni na to, aby nevedli důvěrnou konverzaci na veřejnosti, v otevřené kanceláři a na místech, kde jsou tenké zdi. Informace mohou být ohroženy díky nedostatku bezpečnostního povědomí, neznalosti pravidel a postupů používání odpovídající techniky, například zaslechnutí obsahu hovoru vedeného pomocí mobilního telefonu na veřejných místech, zaslechnutí obsahu zprávy na telefonním záznamníku nebo fax zaslaný omylem nesprávné osobě. Výměna informací a programů bude založena na dohodách uzavřených mezi organizací a externími subjekty.

Je také důležité si uvědomit, že zabezpečení e-mailů a urgentních zpráv, které obsahují osobní zdravotní informace, může zahrnovat procedury pro zdravotnický personál, které nesmí být poskytnuty subjektům péče ani veřejnosti. E-maily mezi odbornými zdravotnickými pracovníky, obsahující osobní zdravotní informace, budou při přenosu zašifrovány. Jednou z možností je použiti digitálních certifikátů.

V následující tabulce jsou uvedeny potřebné zdroje, odpovědnosti a harmonogramy spojené se zaváděním opatření:

Tabulka 16 Opatření 4.2.5.8

Položka	Přímý náklad (odhad)	Odpovědnost	Harmonogram nasazení opatření
Vypracování směrnic pro výměnu informací (včetně mailu)	2500 Kč	Bezp. manažer, administrátor	Do 3 měsíců
Pravidelná bezpečnostní školení	3000 Kč	Bezp. manažer, administrátor	Ihned, 1x za rok
Celkem:	**5500 Kč**		

4.2.5.9 Elektronické zdravotnické informační služby

Měly by být zváženy bezpečnostní dopady a požadavky na opatření spojené s použitím služeb podporujících elektronický obchod, včetně on-line transakcí. Pozornost by měla být věnována ochraně integrity a dostupnosti elektronicky publikovaných informací na veřejně přístupných systémech. Informace přenášené ve veřejných sítích v rámci elektronického obchodování budou chráněny před podvodnými aktivitami, před zpochybňováním smluv, prozrazením či modifikací. Bude zajištěna ochrana informací přenášených při on-line transakcích tak, aby byl zajištěn úplný přenos informací a zamezilo se špatnému směrování, neoprávněné změně zpráv, neoprávněnému prozrazení, neoprávněné duplikaci nebo opakování zpráv.

Kromě těchto pokynů je důležité věnovat pozornost zjištění, zda údaje, obsažené v elektronickém styku a v online transakcích, obsahují osobní zdravotní informace. Pokud ano, musí být tyto informace vhodně chráněny. Ve zdravotní péči je kladen zvláštní důraz na data, vztahující se na vyúčtování (výkonů, péče), medicínské poukazy, faktury za dávky, pohledávky a další data elektronického styku, ze kterých lze odvodit osobní zdravotní informace.

Veřejně dostupné zdravotní informace

Budou archivovány veřejně dostupné zdravotnické informace (na rozdíl od osobních zdravotních informací). Budou chráněna, před neautorizovanou modifikací, integrita veřejně dostupných zdravotnických informací. Bude uveden zdroj (autorství) veřejně dostupných zdravotnických informací a bude chráněna jeho integrita.

Informace publikované na veřejně přístupných systémech budou chráněny proti neoprávněné modifikaci.

V následující tabulce jsou uvedeny potřebné zdroje, odpovědnosti a harmonogramy spojené se zaváděním opatření:

Tabulka 17 Opatření 4.2.5.9

Položka	Přímý náklad (odhad)	Odpovědnost	Harmonogram nasazení opatření
Vytvoření směrnic pro elektronické transakce	2000 Kč	Bezp. manažer	Do 14 dnů
Pravidelná bezpečnostní školení	3000 Kč	Bezp. manažer, administrátor	Ihned, 1x za rok
Celkem:	**5000 Kč**		

4.2.5.10 Monitorování

Cílem je detekovat neoprávněné zpracování informací. Systémy budou monitorovány a bezpečnostní události zaznamenávány. Pro zajištění včasné identifikace problémů informačních systémů bude používán operátorský deník a záznamy předchozích selhání. Veškeré aktivity související s monitorováním a zaznamenáváním událostí budou v souladu s relevantními zákonnými požadavky. Monitorování systému umožňuje kontrolování účinnosti přijatých opatření a ověření souladu s modelem politiky řízení přístupu. Budou stanovena pravidla pro monitorování použití zařízení pro zpracování informací, výsledky těchto monitorování budou pravidelně přezkoumávány. Zařízení

pro zaznamenávání informací a vytvořené záznamy budou vhodným způsobem chráněny proti neoprávněnému přístupu a zfalšování.

Kromě těchto pokynů je důležité poznamenat, že průkazná integrita auditních záznamů může hrát klíčovou roli při soudních vyšetřováních koronery (úředními ohledávači mrtvol), vyšetřování lékařského zanedbání povinné péče a při dalších soudních nebo kvazisoudních řízeních. Jednání odborných zdravotnických pracovníků a načasování událostí jsou někdy určeny v takovýchto (právních) řízeních podrobným zkoumáním změn a aktualizací osobních zdravotních informací jednotlivce.

Aktivity správce systému a systémového operátora budou zaznamenávány. Budou zaznamenány a analyzovány chyby informačních systémů a zařízení a provedena opatření k nápravě. Auditní záznamy budou také obsahovat:

a) identifikátory uživatelů (uživatelská ID);
b) datum, čas a podrobnosti klíčových událostí, např. přihlášení a odhlášení;
c) identifikátor terminálu nebo místa, pokud je to možné;
d) záznam o úspěšných a odmítnutých pokusech o přístup k systému;
e) záznam o úspěšných a odmítnutých pokusech o přístup k datům a jiným zdrojům;
f) změny konfigurace systému;
g) použití oprávnění;
h) použití systémových nástrojů a aplikací;
i) soubory, ke kterým bylo přistupováno a typ přístupu;
j) sítě, ke kterým bylo přistupováno a použité protokoly;
k) alarmy vyvolané systémy pro kontrolu přístupy;
l) aktivaci a deaktivaci ochranných systémů, jako jsou antivirové systémy a systémy pro detekci průniku.

Kromě auditních záznamů se budou zachovávat i záznamy o původním obsahu dat. Hodiny všech důležitých systémů pro zpracování informací by měly být v rámci organizace nebo domény synchronizovány se schváleným zdrojem přesného času. Zdravotnické informační systémy podporující časově kritické sdílené léčebné aktivity musí poskytovat služby časové synchronizace na podporu trasování a „rozpuštění“ časových os aktivit (opětovného ustavení časových rozvrhů činnosti), pokud to bude požadováno.

V následující tabulce jsou uvedeny potřebné zdroje, odpovědnosti a harmonogramy spojené se zaváděním opatření:

Tabulka 18 Opatření 4.2.5.10

Položka	Přímý náklad (odhad)	Odpovědnost	Harmonogram nasazení opatření
Vytvoření záznamů předchozích selhání	500 Kč	Administrátor	Ihned
Monitorování systému	1000 Kč	Administrátor, auditor ISMS	Ihned, 1x za 2 měsíce
Nastavení synchronizace času	500 Kč	Administrátor	Ihned
Celkem:	**2000 Kč**		

4.2.6 Řízení přístupu

Přístup k informacím, zařízením pro zpracování informací a procesům organizace bude řízen na základě provozních a bezpečnostních požadavků. V úvahu se budou brát pravidla organizace pro šíření informací a pravidla, podle nichž probíhá schvalování.

4.2.6.1 Požadavky na řízení přístupu ve zdravotnictví

Bude vytvořena, dokumentována a v závislosti na aktuálních bezpečnostních požadavcích přezkoumávána politika řízení přístupu.

Politika řízení přístupu bude brát v úvahu následující hlediska:

a) bezpečnostní požadavky jednotlivých aplikací organizace;
b) identifikace všech informací ve vztahu k jednotlivým aplikacím a rizika, kterým jsou informace vystaveny;
c) pravidla pro šíření informací a pravidla schvalování, tj. princip oprávněné potřeby znát, bezpečnostní úrovně a klasifikaci informací;
d) konzistence přístupových pravidel a klasifikace informací pro různé systémy a sítě;
e) odpovídající legislativa a ostatní smluvní závazky ve vztahu k ochraně přístupu k datům nebo službám;
f) standardní přístupové profily uživatelů pro běžné kategorie činností;
g) řízení přístupových pravidel v distribuovaném a síťovém prostředí rozeznávajícím všechny možné typy připojení;

h) oddělení jednotlivých rolí pro řízení přístupu, např. vyřizování požadavků na přístup, schvalování přístupu, správa přístupů;
i) požadavky na formální schválení žádostí o přístup;
j) požadavky na pravidelné přezkoumání přístupových práv;
k) odebrání přístupových práv

Je důležité stanovit pravidla na základě principu „Všechno, co není výslovně povoleno, je zakázáno“.

Uživatelé zdravotnických informačních systémů obecně by měli mít přístup k osobním zdravotním informacím, pouze:

a) pokud existuje vztah lékařské péče mezi uživatelem a subjektem dat (subjekt péče, jehož osobní zdravotní informace jsou předmětem přístupu);
b) pokud uživatel provádí činnost jménem subjektu dat;
c) pokud jsou na podporu této činnosti potřebná specifická data.

Kromě těchto pokynů je třeba poznamenat, že aby nedošlo v poskytování zdravotní péče ke zpoždění nebo odmítnutí, existují zde vyšší než obvyklé požadavky na jasnou politiku a postup s odpovídající autorizací s cílem dostat přednost v mimořádných situacích před ‚normálními‘ pravidly přístupu. Zdravotnickým organizacím je doporučeno, aby zvážily zavedení v reálném čase sdílené (federalizované) identity a řešení řízeného v rámci uznání potenciální dodatečné podpory a snížených administrativních nákladů, které toto poskytne politice řízení přístupu. Navíc to podpoří technologie přístupu s vyšší úrovní bezpečnosti, například přístup pomocí čipové karty (smart-card) a jediným přihlášením (single-sign-on).

V následující tabulce jsou uvedeny potřebné zdroje, odpovědnosti a harmonogramy spojené se zaváděním opatření:

Tabulka 19 Opatření 4.2.6.1

Položka	Přímý náklad (odhad)	Odpovědnost	Harmonogram nasazení opatření
Vytvoření směrnic pro řízení přístupu	2000 Kč	Bezp. manažer	Do 1 měsíce
Pravidelné školení o řízení přístupu	3000 Kč	Vedoucí pracovník, bezp. manažer	Ihned, 1x za rok
Celkem:	**5000 Kč**		

4.2.6.2 Řízení přístupu uživatelů

Cílem je zajistit oprávněný přístup uživatelů a předcházet neoprávněnému přístupu k informačním systémům. Budou existovat formální postupy pro přidělování uživatelských práv k informačním systémům a službám. Postupy budou pokrývat všechny fáze životního cyklu přístupu uživatele, od prvotní registrace nového uživatele až po konečné zrušení registrace uživatele, který přístup k informačním systémům a službám již dále nepotřebuje. V případě nutnosti bude věnována zvláštní pozornost potřebě řídit přidělování privilegovaných přístupových oprávnění, která umožňují uživatelům překonat kontroly v systému.

Bude existovat postup pro formální registraci uživatele včetně jejího zrušení, který zajistí autorizovaný přístup ke všem víceuživatelským informačním systémům a službám. Postup pro registraci a uživatele a jejího zrušení bude zahrnovat:

a) použití unikátního uživatelského identifikátoru (ID), aby bylo možné propojit uživatele s jím provedenými akcemi, a zajistit tak jejich odpovědnost. Použití skupinového ID by mělo být povoleno pouze tam, kde to je nezbytné pro určitou práci, použití by mělo být chváleno a dokumentováno;
b) kontrolu toho, že uživatel má oprávnění používat informační systém nebo služby od vlastníka systému. Vhodný může být také zvláštní souhlas s přístupovými právy od nadřízených uživatele;
c) kontrolu toho, že úroveň přiděleného přístupu odpovídá záměrům organizace a je shodná s bezpečnostní politikou organizace, například není v rozporu s principem oddělení povinností;
d) předání dokumentu vymezujícího přístupová práva jednotlivým uživatelům;
e) požadavek na uživatele, aby podepsali prohlášení, že rozumí podmínkám přístupu;
f) zajištění toho, aby poskytovatelé služeb neumožnili přístup, dokud nebude proces autorizace dokončen;
g) udržování formálního záznamu o všech registrovaných osobách oprávněných využívat službu;
h) ihned odebrat přístupová práva uživatelům, kteří změnili pracovní místo nebo opustili organizaci;
i) pravidelně kontrolovat a odstranit již dále nepotřebné ID uživatelů a jejich účty;

j) zajistit, aby již nepotřebné ID uživatelů nebyly přiděleny jiným uživatelům.

Přidělování hesel bude řízeno formálním procesem. Proces bude vyhovovat následujícím požadavkům:

a) vyžadovat od uživatelů podpis prohlášení, že se zavazují k držení svých hesel v tajnosti a k zachování hesel pracovní skupiny pouze mezi jejími členy (to může být začleněno v pracovních podmínkách);
b) zajistit, aby v případě, že si uživatelé sami mění své heslo, dostali na počátku bezpečné jednorázové heslo, které jsou nuceni ihned po přihlášení změnit;
c) zavést postupy jednoznačné identifikace uživatelů předtím než jim je poskytnuto nové, náhradní anebo dočasné heslo;
d) dočasně přidělená hesla by měla být jedinečná a neměla by být lehce uhodnutelná;
e) uživatelé budou muset potvrdit přijetí hesel;
f) hesla by nikdy neměla být v počítači uložena v nechráněné podobě;
g) dodavateli přednastavená hesla budou muset být ihned po instalaci systému nebo aplikačního programového vybavení změněna;

Je třeba poznamenat, že časová tíseň při poskytování lékařské péče může ztížit efektivní použití hesel. Mnoho zdravotnických organizací zvažuje přijmout pro vyřešení tohoto problému alternativní autentizační technologie.

Vedení organizace bude v pravidelných intervalech provádět formální přezkoumání přístupových práv uživatelů.

Kromě těchto pokynů je třeba věnovat zvláštní pozornost těm uživatelům, u kterých se rozumně předpokládá, že budou poskytovat pohotovostní službu, protože mohou potřebovat přístup k osobním zdravotním informacím v pohotovostních situacích, kdy předmět péče nemusí být schopen sdělit souhlas.

V následující tabulce jsou uvedeny potřebné zdroje, odpovědnosti a harmonogramy spojené se zaváděním opatření:

Tabulka 20 Opatření 4.2.6.2

Položka	Přímý náklad (odhad)	Odpovědnost	Harmonogram nasazení opatření
Přidělování uživatelských práv	0 Kč	Administrátor	Ihned
Kontrola přístupových oprávnění	500 Kč	Administrátor	Ihned, 1x za 6měsíců
Vytvoření záznamu o všech registrovaných uživatelích	500 Kč	Administrátor	Ihned
Celkem:	**1000 Kč**		

4.2.6.3 Odpovědnosti uživatelů

Cílem je předcházet neoprávněnému uživatelskému přístupu, prozrazení nebo krádeži informací a prostředků pro zpracování informací. Pro účinné zabezpečení je nezbytná spolupráce oprávněných uživatelů. Uživatelé by si měli být vědomi odpovědnosti za dodržování účinných opatření kontroly přístupu, zejména s ohledem na používání hesel, a bezpečnosti jim přidělených prostředků. Pro snížení rizika neoprávněného přístupu (nebo poškození) k dokumentům, médiím a prostředkům pro zpracování informací, bude zavedena zásada prázdného stolu a prázdné obrazovky monitoru. Tím by se mělo odstranit známé bezpečnostní riziko, kdy si uživatelé píší hesla na papírky na monitor.

Při výběru a používání hesel bude po uživatelích požadováno, aby dodržovali stanovené bezpečnostní postupy. Všichni uživatelé budou obeznámeni s tím, že:

a) hesla se udržují v tajnosti;
b) hesla nesmí být zaznamenána (např. na papíře, v souborech nebo v přenosných zařízeních), s výjimkou jejich bezpečného uložení, a když byl způsob jejich uložení schválen;
c) hesla se musí změnit v případě jakéhokoliv náznaku možného kompromitování systému nebo hesla;
d) heslo by mělo být kvalitní, mělo by mít minimální délku šest znaků, a to tak, aby:
    a. bylo dobře zapamatovatelné;

b. nebylo založeno na informacích vztahujících se k osobě, které by mohl kdokoliv další lehce uhodnout nebo získat, například jména, telefonní čísla, data narození apod.;
c. nebylo zranitelné při použití slovníkových útoků (nemělo by se skládat ze slov vyskytujících se ve slovnících);
d. neobsahovalo po sobě jdoucí stejné znaky a neobsahovalo pouze číselné nebo pouze písmenné skupiny.

e) musí měnit hesla v pravidelných intervalech nebo na základě počtu přihlášení (hesla pro privilegovaný přístup by se měla měnit častěji než normální hesla) a vyhýbat se opakovanému použití nebo opakování starých hesel;
f) musí změnit dočasná hesla při prvním přihlášení;
g) nebudou zahrnovat hesla do žádného automatizovaného přihlašovacího procesu, například uložení do makra nebo funkční klávesy;

Zvláštní péče bude také věnována help-desku, který řeší ztracená a zapomenutá hesla a může se také stát cílem útoku.

Uživatelům bude doporučeno:

a) při ukončení práce ukončit aktivní relace nebo je zajistit vhodným mechanizmem, například spořičem obrazovky s heslem;
b) odhlásit se v případě ukončení relace od sálových počítačů, serverů a kancelářských PC (tj. nevypínat pouze monitor počítače);
c) pokud se nepoužívají, zabezpečit PC nebo terminály pomocí uzamčení klávesnice nebo ekvivalentní kontroly, například přístupovým heslem.

Dále bude přijata zásada prázdného stolu ve vztahu k dokumentům a vyměnitelným médiím a zásada prázdné obrazovky monitoru u prostředků pro zpracování informací.

V následující tabulce jsou uvedeny potřebné zdroje, odpovědnosti a harmonogramy spojené se zaváděním opatření:

Tabulka 21 Opatření 4.2.6.3

Položka	Přímý náklad (odhad)	Odpovědnost	Harmonogram nasazení opatření
Pravidelná bezpečnostní školení	3000 Kč	Bezp. manažer, administrátor	Ihned, 1x za rok
Tvorba směrnic o politice hesel	2000 Kč	Bezp. manažer, administrátor	Do 2 měsíců
Celkem:	**5000 Kč**		

4.2.6.4 Řízení přístupu k síti

Cílem je předcházet neautorizovanému přístupu k síťovým službám. Přístup k interním i externím síťovým službám bude řízen. Je to nezbytné pro zajištění toho, aby uživatelé mající přístup k sítím nebo síťovým službám neohrožovali bezpečnost těchto služeb.

K tomu je potřeba:

a) vhodné rozhraní sítě organizace se sítěmi jiných organizací nebo veřejnými sítěmi;
b) odpovídající autentizační mechanizmus pro uživatele a zařízení;
c) řízení přístupu uživatelů k informačním službám.

Uživatelé budou mít přímý přístup pouze k těm síťovým službám, pro jejichž použití byli zvlášť oprávněni. Přístup vzdálených uživatelů bude autentizován. Autentizace vzdálených uživatelů může být zajištěna například použitím kryptografických technik, autentizačních předmětů (hardware token) nebo protokolem typu výzva/odpověď (challenge/response). Implementaci takovýchto technik například využívají virtuální privátní sítě (VPN sítě). Pro kontrolu identity zdroje komunikace může být také použito vyhrazené soukromé linky nebo prostředků pro ověření síťové adresy uživatele. Pro bezpečný přístup k bezdrátovým sítím budou implementovány dodatečné techniky autentizace. Je to z důvodu vyššího rizika narušení komunikace nebo vložení falešné zprávy než je tomu u sítí klasických.

Pro autentizaci připojení z vybraných lokalit a přenosných zařízení bude vynucena automatická identifikace zařízení. Automatická identifikace zařízení je způsob, který se uplatňuje, jestliže je důležité, aby byla komunikace iniciována pouze z určité lokality nebo zařízení.

Fyzický i logický přístup k diagnostickým a konfiguračním portům bude bezpečně řízen. Porty, služby a obdobná zařízení instalovaná na počítačích nebo síťových zařízeních, pokud nejsou pro organizaci potřebné, budou zakázány nebo odstraněny. Mnoho počítačových, síťových a komunikačních systémů obsahuje prostředky pro vzdálenou konfiguraci a diagnostický přístup, které využívá podpůrný personál pro údržbu systému. Pokud jsou nechráněny, představují diagnostické porty prostředek k neoprávněnému přístupu.

Skupiny informačních služeb, uživatelů a informačních systémů budou v sítích odděleny. Jedna z metod správy bezpečnosti velkých sítí je rozdělení sítí do separátních

logických domén, tj. vnitřních síťových domén organizace a externích síťových domén, kde každá z nich je chráněna definovaným bezpečnostním perimetrem. V rámci logických domén mohou být pro další bezpečné oddělení síťových prostředí (např. veřejně přístupné systémy, vnitřní sítě a kritická aktiva) uplatněny silnější skupiny opatření. Oddělené domény mohou být vytvořeny na základě řízení toku dat s využitím možností směrování a přepínání, jako například nastavení ACL (Access Control List). Oddělení v sítích bude založeno na klasifikaci ukládaných a zpracovávaných informací, úrovni důvěry a typu činností, kterými se organizace zabývá tak, aby byl v případě narušení služeb minimalizován celkový dopad na organizaci. Bude zváženo oddělení bezdrátových sítí od interních a privátních sítí.

U sdílených sítí, zejména těch, které přesahují hranice organizace, budou omezeny možnosti připojení uživatelů. Omezení budou v souladu s politikou řízení přístupu a s požadavky aplikací. Příklady aplikací, na které budou nasazena omezení, jsou:

a) odesílání zpráv, např. elektronická pošta;
b) přenos souborů;
c) interaktivní přístup;
d) přístup k aplikacím.

Bude zváženo omezení přístupu k síti na určitou denní dobu nebo datum.

Pro zajištění toho, aby počítačová spojení a informační toky nenarušovaly politiku řízení přístupu aplikací organizace, bude zavedeno řízení směrování sítě. Řízení směrování bude založeno na ověření zdrojové a cílové adresy. V následující tabulce jsou uvedeny potřebné zdroje, odpovědnosti a harmonogramy spojené se zaváděním opatření:

Tabulka 22 Opatření 4.2.6.4

Položka	Přímý náklad (odhad)	Odpovědnost	Harmonogram nasazení opatření
Pravidelná bezpečnostní školení	3000 Kč	Bezp. manažer, administrátor	Ihned, 1x za rok
Tvorba směrnic o přístupu k síti	2000 Kč	Bezp. manažer, správce sítě	Do 2 měsíců
Monitoring přístupu k síti	500 Kč	Správce sítě	Ihned, 1x za měsíc
Celkem:	**5500 Kč**		

4.2.6.5 Řízení přístupu k operačnímu systému

Cílem je předcházet neautorizovanému přístupu k operačním systémům.

Pro omezení přístupu k prostředkům počítače budou použity bezpečnostní prostředky na úrovni operačního systému. Tyto prostředky budou schopné:

a) autentizace oprávněných uživatelů v souladu se stanovenou politikou řízení přístupu;
b) zaznamenávat úspěšné a neúspěšné pokusy o autentizaci;
c) zaznamenávat využití systémových privilegií;
d) spouštět varování při porušení systémových bezpečnostních politik;
e) poskytovat vhodné prostředky pro autentizaci;
f) v případě potřeby omezit dobu připojení uživatele.

Dobrý přihlašovací postup by měl omezit počet povolených neúspěšných přihlašovacích pokusů (doporučují se tři pokusy) a zároveň zvážit:

a) zaznamenání neúspěšných pokusů;
b) povolení dalšího pokusu o přihlášení až za určitou dobu nebo odmítnutí dalších pokusů bez dalšího specifického potvrzení;
c) odpojení všech spojení na data;
d) zasílání varovných zpráv do systémové konzole (správci sítě) v případě, že je překročen maximální počet pokusů o přihlášení;

Také by měl nezobrazovat heslo při jeho zadávání anebo jej maskovat použitím zástupných symbolů. Všichni uživatelé budou mít pro výhradní osobní použití jedinečný identifikátor (uživatelské ID), bude také zvolen vhodný způsob autentizace k ověření jejich identity. Uživatelská ID budou umožňovat pozdějšího vysledování odpovědnosti konkrétních osob za činnosti v systému. Běžné aktivity uživatelů by neměly být prováděny z privilegovaných účtů. Pro identifikaci a autentizaci mohou být také použity předměty, které jsou vlastnictvím uživatelů, jako například paměťové nebo čipové karty. Pro autentizaci identity osoby mohou být použity také biometrické autentizační technologie, využívající unikátní osobní charakteristiky nebo rysy. Kombinace bezpečného propojení technologií a mechanizmů přináší kvalitnější autentizaci. Neaktivní relace by měly se po stanovené době nečinnosti ukončit.

V následující tabulce jsou uvedeny potřebné zdroje, odpovědnosti a harmonogramy spojené se zaváděním opatření:

Tabulka 23 Opatření 4.2.6.5

Položka	Přímý náklad (odhad)	Odpovědnost	Harmonogram nasazení opatření
Pravidelná bezpečnostní školení	3000 Kč	Bezp. manažer, administrátor	Ihned, 1x za rok
Tvorba směrnic o používání operačních systémů	2000 Kč	Bezp. manažer, administrátor	Do 2 měsíců
Celkem:	**5000 Kč**		

4.2.6.6 Řízení přístupu k aplikacím a informacím

Cílem je předcházet neoprávněnému přístupu k informacím uloženým v počítačových systémech. Pro omezení přístupu k aplikačním systémům budou použity bezpečnostní prostředky. Logický přístup k programům a informacím bude omezen na oprávněné uživatele. Aplikační systémy by měly:

a) kontrolovat přístup uživatelů k datům a funkcím aplikačního systému v souladu s definovanou politikou řízení přístupu;
b) poskytovat ochranu před neoprávněným přístupem ke všem nástrojům a systémovým programům, které mohou obejít systémové a aplikační kontrolní mechanizmy;
c) nenarušit bezpečnost jiných systémů, se kterými jsou sdíleny informační zdroje.

Uživatelé aplikačních systémů, včetně pracovníků podpory, budou mít přístup k informacím a funkcím aplikačních systémů omezen v souladu s definovanou politikou řízení přístupu. Citlivé aplikační systémy budou mít oddělené (izolované) počítačové prostředí. Zdravotnické informační systémy zpracovávající osobní informace musí autentizovat uživatele a měly by to provést pomoci autentizace obsahující alespoň dva různé faktory.

Kromě těchto pokynů je třeba věnovat zvláštní pozornost technickým opatřením, pomocí kterých je subjekt péče bezpečně autentizován, když přistupuje ke všem nebo k části svých vlastních informací (v těch zdravotnických informačních systémech, které takový přístup umožňují). Podobný důraz by měl být kladen na snadnost používání

těchto opatření zejména pro subjekty s handicapem a na zajištění přístupu opatrovníkům těchto subjektů (náhradní jednotlivci, kteří rozhodují).

V následující tabulce jsou uvedeny potřebné zdroje, odpovědnosti a harmonogramy spojené se zaváděním opatření:

Tabulka 24 Opatření 4.2.6.6

Položka	Přímý náklad (odhad)	Odpovědnost	Harmonogram nasazení opatření
Pravidelná bezpečnostní školení	3000 Kč	Bezp. manažer, administrátor	Ihned, 1x za rok
Tvorba směrnic o používání zdravotnických aplikací	2000 Kč	Administrátor	Do 2 měsíců
Kontrola uživatelských přístupů	500 Kč	Administrátor	Ihned, 1x za měsíc
Celkem:	**5500 Kč**		

4.2.6.7 Mobilní provádění výpočtů a práce na dálku

Cílem je zajistit bezpečnost informací při použití mobilní výpočetní techniky a při využití zařízení pro práci na dálku.

Požadovaná ochrana bude odpovídat rizikovosti těchto specifických způsobů práce. Při použití mobilních výpočetních prostředků bude zváženo riziko práce v nechráněném prostředí a bude zajištěna vhodná ochrana. V případě práce na dálku by měla být zavedena ochrana na místě výkonu práce a měly by být zajištěny vhodné podmínky pro tento způsob práce.

Budou ustavena formální pravidla a přijata opatření na ochranu proti rizikům použití mobilních výpočetních a komunikačních prostředků. Budou přijata taková formální pravidla, která berou v úvahu riziko práce s mobilním výpočetním zařízením například notebooky a mobilní telefony. Tyto pravidla budou zahrnovat například požadavky na fyzickou ochranu, kontrolu přístupu, kryptografické techniky, zálohování a antivirovou ochranu. Mobilní síťová bezdrátová připojení, jakkoliv podobná sítím s připojením po drátech, mají z pohledu bezpečnosti určité významné rozdíly. Stále se používají některé bezdrátové šifrovací protokoly, například WEP (Wired Equivalent Privacy) i přes známá slabá místa, která je činí značnou měrou neúčinnými. Kromě toho informace uložené na mobilních zařízeních není možné vždy zálohovat (například

z důvodu omezené šířky pásma sítě nebo proto, že zařízení nejsou v době plánovaného zálohováni připojena).

Aby bylo dosaženo povědomí o dalších rizicích tohoto způsobu práce a opatřeních, která budou zavedena, měla by být pro personál, používající mobilní zařízení, organizována školení.

Organizace vytvoří a do praxe zavede zásady, operativní plány a postupy pro práci na dálku.

Organizace schválí aktivity práce na dálku pouze tehdy, jestliže jsou splněny odpovídající bezpečnostní požadavky a jsou zavedena opatření, jež jsou v souladu s bezpečnostní politikou organizace. Na vzdáleném pracovišti by měla existovat vhodná ochrana například proti zcizení zařízení a informací, neautorizovanému vyzrazení informací, neautorizovanému vzdálenému přístupu k vnitřním systémům organizace nebo zneužití prostředků.

V následující tabulce jsou uvedeny potřebné zdroje, odpovědnosti a harmonogramy spojené se zaváděním opatření:

Tabulka 25 Opatření 4.2.6.7

Položka	Přímý náklad (odhad)	Odpovědnost	Harmonogram nasazení opatření
Pravidelná bezpečnostní školení	3000 Kč	Bezp. manažer, administrátor	Ihned, 1x za rok
Tvorba směrnic o používání mobilních zařízení a o práci na dálku	2500 Kč	Administrátor	Do 3 měsíců
Celkem:	**5500 Kč**		

4.2.7 Akvizice, vývoj a údržba informačních systémů

Cílem je zajistit, aby se bezpečnost stala neodlučitelnou součástí informačních systémů. To zahrnuje provozní systémy, infrastrukturu, interní aplikace organizace, zakoupené produkty, služby a uživatelsky vyvinuté aplikace. Návrh a implementace informačního systému na podporu procesů organizace může být z hlediska bezpečnosti kritický. Bezpečnostní požadavky by měly být stanoveny a odsouhlaseny ještě před zahájením vývoje informačního systému. Všechny bezpečnostní požadavky by měly být v projektu stanoveny již ve fázi definice požadavků a měly by být zdůvodněny, odsouhlaseny a dokumentovány jako součást vývoje informačního systému.

Požadavky organizace na nové informační systémy nebo na rozšíření existujících systémů budou obsahovat také požadavky na bezpečnostní opatření. Tato specifikace bude brát v úvahu začlenění automatizovaných kontrol do systému, ale i potřebu doplňujících manuálních kontrol. Stejně se bude postupovat i při testování, vytvořených nebo zakoupených, programových balíků aplikací organizace. U zakoupených produktů by měl nejprve následovat formální proces testování a zavedení do provozu. Ve smlouvách s dodavateli budou specifikovány požadavky na bezpečnost.

4.2.7.1 Bezchybné zpracování v aplikacích

Cílem je předcházet chybám, ztrátě, modifikaci nebo zneužití uživatelských dat v aplikacích. Pro zajištění bezchybného zpracování budou do aplikačních systémů, včetně těch, které jsou vytvořeny uživatelsky, zahrnuty vhodné kontroly. Budou zahrnovat potvrzení platnosti vstupních dat, interního zpracování a výstupních dat. Přijetí dodatečných kontrol bude zváženo u systémů, které zpracovávají nebo mají vliv na zpracování citlivých, cenných nebo kritických informací. Vstupní data aplikací budou kontrolována z hlediska správnosti a adekvátnosti. Pro detekci jakéhokoliv poškození nebo modifikace informací vzniklého chybami při zpracování nebo úmyslnými zásahy, bude zváženo začlenění kontroly platnosti dat. U jednotlivých aplikací budou stanoveny bezpečnostní požadavky na zajištění autentizace a integrity zpráv, dle potřeby určena a zavedena vhodná opatření. Pro zajištění toho, že zpracování uložených informací je bezchybné a odpovídající dané situaci, bude provedeno ověření platnosti výstupních dat.

Zdravotnické informační systémy, zpracovávající osobní zdravotní informace, musí:

a) zajistit, aby byl každý subjekt péče v rámci systému jednoznačně identifikován;

b) být schopny slučovat duplicitní či vícenásobné záznamy, zjistí-li se, že vícenásobné záznamy pro stejný subjekt péče byly vytvořeny neúmyslně nebo v průběhu lékařské pohotovosti.

Při poskytování naléhavé péče a v dalších situacích, kdy není možné adekvátně identifikovat subjekty péče, nevyhnutelně dochází k případům vytvoření více záznamů

stejného pacienta. V každém zdravotnickém informačním systému musí existovat nějaká možnost pro sloučení více případů pacientových záznamů do jediného záznamu.

Takové sloučení vyžaduje maximální péči a kromě personálu, který je pro sloučení záznamů proškolený, může také vyžadovat technické nástroje pro usnadnění začlenění informací z původních záznamů do jednotného celku.

Organizace zajistí, aby data, ze kterých je možné odvodit osobní identifikaci, byla uchována pouze, je-li to nutné, a aby techniky pro vymazání, anonymizaci a pseudonymizaci byly používány v plném rozsahu s cílem minimalizovat riziko neúmyslného zpřístupňování osobních informací.

Zdravotnické informační systémy zpracovávající osobní zdravotní informace musí poskytovat osobní identifikační informace, které pomohou odborným zdravotnickým pracovníkům potvrdit, že se získaný elektronický zdravotnický záznam shoduje se subjektem péče podstupujícím léčbu.

Kromě těchto pokynů je potřeba zvážit některé další důležité faktory. Předtím, než se zdravotní profesionálové spolehnou na osobní zdravotní informace poskytované zdravotnickým informačním systémem, musí mít dostatek informací k ujištění, že se subjekt péče, kterému je péče poskytována, shoduje se získanými informacemi. Porovnání léčeného subjektu péče s již existujícím záznamem může být nesnadný úkol.

Některé systémy zvyšují bezpečnost přiložením fotografického ID ke každému záznamu subjektu péče. Takováto vylepšení samotná však mohou způsobit problémy narušení soukromí, protože potenciálně umožňují zachycení implicitních obličejových charakteristik, jako například rasa, které nejsou zahrnuty v datových polích. Požadavky na identifikaci subjektů péče a dostupnost dat používaných k její podpoře se také mohou lišit od jurisdikce k jurisdikci. Navrhování zdravotnických informačních systémů je nutné věnovat velkou péči, aby odborní zdravotní pracovníci mohli důvěřovat systému, že jim poskytne informace potřebné k potvrzení, že každý vyhledaný záznam odpovídá osobě podstupující léčbu.

Zdravotnické informační systémy by měly umožnit ověření, zda jsou vytištěné sestavy kompletní (například „strana 3 z 5“).

V následující tabulce jsou uvedeny potřebné zdroje, odpovědnosti a harmonogramy spojené se zaváděním opatření:

Tabulka 26 Opatření 4.2.7.1

Položka	Přímý náklad (odhad)	Odpovědnost	Harmonogram nasazení opatření
Zahrnutí kontrol aplikačních systémů včetně platnosti dat	2000 Kč	Administrátor, bezp. manažer	Do 6 měsíců
Nastavit pravidla pro zdravotnické informační systémy včetně pseudonymizace	5000 Kč	Administrátor, programátor IS	Do 6 měsíců
Celkem:	**7000 Kč**		

4.2.7.2 Kryptografická opatření

Cílem je ochránit důvěrnost, autentičnost a integritu informací s pomocí kryptografických prostředků.

Budou vytvořena pravidla pro použití kryptografických opatření. K podpoře používání kryptografických technik bude v organizaci existovat systém jejich správy.

Při vytváření pravidel bude zváženo následující:

a) manažerský přístup k zavedení kryptografických opatření v celé organizaci, včetně základních principů, podle kterých by měly být informace chráněny;
b) na základě výsledků hodnocení rizik by měla být stanovena požadovaná úroveň ochrany a to s ohledem na typ, sílu a kvalitu požadovaného šifrovacího algoritmu;
c) použití šifrování na ochranu citlivých informací při přenosu na mobilních nebo vyměnitelných počítačových médiích a zařízení anebo komunikačními linkami;
d) přístup ke správě klíčů, včetně metod řešení ochrany šifrovacích klíčů, obnovení šifrovaných informací v případě ztráty, vyzrazení nebo poškození klíčů;
e) úlohy a odpovědnosti, například kdo je odpovědný za:
    a. implementaci pravidel;
    b. správu klíčů včetně jejich generování;
f) normy, které budou přijaty, aby implementace opatření v celé organizaci byla účinná (pro které procesy budou použita která řešení)
g) dopad, jaký má šifrování informací na prováděné kontroly obsahu (např. detekce virů).

Tato pravidla jsou potřebná, aby bylo možno maximalizovat výhody a minimalizovat rizika z použití kryptografických metod a také pro vyvarování se nevhodného nebo nesprávného použití. Při použití digitálních podpisů bude brán zřetel na všechny relevantní právní úpravy, které stanovují podmínky vážící se k právní závaznosti digitálních podpisů.

Na podporu používání kryptografických technik v organizaci by měl existovat systém jejich správy.

Všechny klíče budou chráněny před modifikací a zničením. Tajné a soukromé klíče je třeba chránit proti neautorizovanému prozrazení. Pro zabezpečení prostředků určených ke generování, ukládání a archivaci klíčů budou použity prostředky fyzické ochrany. Současně s bezpečnou správou tajných a privátních klíčů bude zvážena i ochrana veřejných klíčů. Autentizace veřejných klíčů se zpravidla řeší certifikáty veřejných klíčů, které jsou vydávány certifikační autoritou. Ta by měla být uznávanou organizací a pro zajištění požadovaného stupně důvěryhodnosti by měla mít zavedena vhodná opatření a postupy.

Obsah dohod o úrovni služeb nebo smluv s externím poskytovatelem kryptografických služeb, například s certifikační autoritou, bude pokrývat právní závaznost, spolehlivost a dobu odezvy zajišťovaných služeb.

Existuje hrozba, že někdo padělá digitální podpis výměnou veřejného klíče uživatele za svůj veřejný klíč. Tento problém se řeší zejména certifikáty veřejných klíčů.

V následující tabulce jsou uvedeny potřebné zdroje, odpovědnosti a harmonogramy spojené se zaváděním opatření:

Tabulka 27 Opatření 4.2.7.2

Položka	Přímý náklad (odhad)	Odpovědnost	Harmonogram nasazení opatření
Nasazení kryptografických technik	10000 Kč	Administrátor, bezp. manažer	Do 12 měsíců
Školení osob pracujících s šifrovaným obsahem	3000 Kč	Administrátor	Ihned, 1x za 1 rok
Celkem:	**13000 Kč**		

4.2.7.3 Bezpečnost systémových souborů

Cílem je zajistit bezpečnost systémových souborů. Přístup k systémovým souborům a zdrojovým kódům programů bude řízen, projekty IT a podpůrné činnosti budou prováděny bezpečným způsobem. Budou přijata opatření zabraňující prozrazení citlivých informací v testovacím prostředí.

Budou zavedeny postupy kontroly instalace programového vybavení na provozních systémech. Aktualizace provozního programového vybavení, aplikací a knihoven programů budou prováděny pouze oprávněným správcem na základě schválení vedením. Provozní systémy budou obsahovat pouze spustitelný kód. Provozní systémy by neměly obsahovat vývojový kód nebo kompilátory. Budou udržovány auditní záznamy všech aktualizací provozních programových knihoven. Pro případ nouze budou uchovány předcházející verze programového vybavení. Každé rozhodnutí o povýšení verze bude brát v úvahu její bezpečnost, tj. její nové bezpečnostní vlastnosti nebo počet, a závažnost bezpečnostních problémů s ní spojených. V případě, že existují opravné dávky (záplaty) pro programové vybavení, které mohou pomoci odstranit nebo redukovat bezpečnostní slabiny, budou použity co nejdříve. Provozní systémy by měly být aktualizovány pouze v případech, kdy existuje takový požadavek, například pokud stávající verze operačního systému již nestačí aktuálním požadavkům organizace. Aktualizace by neměly probíhat jen proto, že je k dispozici nová verze operačního systému.

Testovací data budou pečlivě vybrána, chráněna a kontrolována. Organizace nebude používat aktuální osobní zdravotní informace jako testovací data. Přístup ke knihovně zdrojových kódů bude omezen.

V následující tabulce jsou uvedeny potřebné zdroje, odpovědnosti a harmonogramy spojené se zaváděním opatření:

Tabulka 28 Opatření 4.2.7.3

Položka	Přímý náklad (odhad)	Odpovědnost	Harmonogram nasazení opatření
Opatření zabraňující prozrazení citlivých informací v testování	2500 Kč	Bezp. manažer, vedoucí programátorů IS	Do 12 měsíců
Nastavení pravidel pro aktualizace a kontroly integrity OS	1000 Kč	Administrátor	Do 3 měsíců
Celkem:	**3500 Kč**		

4.2.8 Zvládání bezpečnosti incidentů

Cílem je zajistit nahlášení bezpečnostních událostí a slabin informačního systému způsobem, který umožní včasné zahájení kroků vedoucích k nápravě. Budou ustaveny formální postupy pro hlášení bezpečnostních událostí a pro zvyšování stupně jejich důležitosti. Všichni zaměstnanci, smluvní strany a uživatelé třetích stran by měli znát postupy hlášení různých typů událostí a slabin, které mohou mít dopad na bezpečnost aktiv organizace. Zjištěné bezpečnostní události a slabiny budou zaměstnanci ihned hlásit na určené místo.

4.2.8.1 Hlášení bezpečnostních událostí a slabých míst

Bezpečnostní události budou hlášeny příslušnými řídícími cestami tak rychle, jak je to jen možné. Pro hlášení bezpečnostní události bude vytvořen formalizovaný postup, včetně postupu reakce na incidenty a jejich eskalace (zvýšení stupně důležitosti), definující činnosti, které budou po přijetí hlášení provedeny. Pro hlášení bezpečnostních událostí bude zřízeno kontaktní místo, tzv. help-desk. Kontaktní místo bude známo všem zaměstnancům organizace, bude vždy k dispozici a mělo by vždy zajistit přiměřenou a včasnou reakci. Postupy hlášení by měly zahrnovat:

a) vytvoření procesu zajišťujícího přiměřenou zpětnou vazbu, aby ten, kdo nahlásí incident, byl informován o výsledcích vyšetřování incidentu a jeho uzavření;
b) formuláře podporující proces hlášení bezpečnostních událostí a zároveň zajišťující, že hlášení bude splňovat veškeré nezbytné kroky (napomáhající osobě, která incident hlásí, provést všechny nezbytné kroky);
c) nastavení správného chování v případě bezpečnostní události, např.
    a. okamžité zaznamenání všech důležitých detailů (např. typ nesouladu nebo narušení, chybné fungování, hlášky na obrazovce, podivné chování);
    b. za žádných okolností neprověřovat bezpečnostní události, ale okamžitě je hlásit na určené místo;
d) odkaz na zavedená formalizovaná pravidla pro disciplinární řízení se zaměstnanci, smluvními stranami nebo uživateli třetích stran, kteří způsobili narušení bezpečnosti.

Všichni zaměstnanci, smluvní strany a další nespecifikovaní uživatelé informačního systému a služeb budou povinni zaznamenat a hlásit jakékoliv bezpečnostní slabiny nebo podezření na bezpečnostní slabiny v systémech nebo službách. Zaměstnancům, smluvním stranám a uživatelům třetích stran bude doporučeno, aby se nepokoušeli podezřelé slabiny sami prověřovat. Testování bezpečnostních slabin může být interpretováno jako potenciální zneužití systému. Mimo to může testování slabin také způsobit narušení informačního sytému nebo služby a vyústit až v podniknutí příslušných právních kroků proti osobě, která testování provedla.

V následující tabulce jsou uvedeny potřebné zdroje, odpovědnosti a harmonogramy spojené se zaváděním opatření:

Tabulka 29 Opatření 4.2.8.1

Položka	Přímý náklad (odhad)	Odpovědnost	Harmonogram nasazení opatření
Vytvoření help-desku	5000 Kč	Administrátor, bezp. manažer	Do 1 měsíce
Školení postupu hlášení bezpečnostních incidentů	2000 Kč	Administrátor	Ihned, 1x za rok
Celkem:	**7000 Kč**		

4.2.8.2 Hlášení bezpečnostních incidentů

Pro potřeby nově vzniklé prováděcí vyhlášky ke kybernetickému zákonu uvádím vzorový formulář v příloze.

4.2.8.3 Řízení bezpečnostních incidentů a zlepšování

Cílem je zajistit odpovídající a účinný přístup ke zvládání bezpečnostních incidentů. Pro účinné zvládání bezpečnostních útoků a slabin budou stanoveny odpovědnosti a zavedeny formalizované postupy umožňující okamžitou reakci. Bude nastaven proces neustálého zlepšování reakce, monitorování, vyhodnocování a celkového zvládání bezpečnostních incidentů. Pro zajištění souladu s právními požadavky budou v případech, kdy je to vyžadováno, shromážděny důkazy. Postupy zvládání bezpečnostních incidentů budou odsouhlaseny vedením a bude zajištěno, aby zodpovědné osoby byly obeznámeny s nastavenými prioritami pro zvládání bezpečnostních incidentů. Informace získané při vyhodnocení bezpečnostních incidentů budou využity pro identifikaci opakujících se incidentů nebo incidentů s velkými

následky. Závěry z vyhodnocení bezpečnostních incidentů mohou také signalizovat potřebu využití dodatečných nebo důkladnějších opatření, která by omezila frekvenci, škody a náklady jejich budoucích výskytů. Kromě toho budou brány v úvahu při revizi bezpečnostní politiky. V případech, kdy vyústění bezpečnostního incidentu směřuje k právnímu řízení (dle práva občanského nebo trestního) vůči osobě anebo organizaci, by měly být sbírány, uchovávány a soudu předkládány důkazy v souladu s pravidly příslušné jurisdikce, kde se bude případ projednávat.

V následující tabulce jsou uvedeny potřebné zdroje, odpovědnosti a harmonogramy spojené se zaváděním opatření:

Tabulka 30 Opatření 4.2.8.3

Položka	Přímý náklad (odhad)	Odpovědnost	Harmonogram nasazení opatření
Zavedení formalizovaných postupů pro reakci na incidenty	3000 Kč	Bezp. manažer, koordinátor řízení kontinuity činností	Do 1 měsíce
Celkem:	**3000 Kč**		

4.2.9 Aspekty řízení kontinuity činností organizace z hlediska bezpečnosti informací

Cílem je bránit přerušení provozních činností a chránit kritické procesy organizace před následky závažných selhání informačních systémů nebo katastrof a zajistit jejich včasnou obnovu.

Pro minimalizaci následků a zotavení se ze ztráty informačních aktiv (které může být např. výsledkem přírodních pohrom, nehod, chyb zařízení a úmyslného jednání) na přijatelnou úroveň, za pomoci preventivních a zotavovacích opatření, bude zaveden proces řízení kontinuity činností organizace. Tento proces bude identifikovat kritické činnosti organizace a začleňovat požadavky řízení bezpečnosti informací s ohledem na požadavky provozní, personální, materiální, dopravní a požadavků na zařízení. Důsledky pohrom, bezpečnostních chyb a ztráty dostupnosti služeb budou identifikovány v rámci analýzy dopadů. Pro zajištění toho, aby mohly být obnoveny klíčové činnost organizace v požadovaných lhůtách, je vhodné připravit a implementovat plány kontinuity. Bezpečnost informací se stane nedílnou součástí

procesu řízení kontinuity činností a dalších řídících procesů v rámci organizace. Řízení kontinuity činností organizace bude zahrnovat opatření k identifikaci a minimalizaci rizik, omezovat důsledky škodlivých incidentů a zajistí včasnou dostupnost informací potřebných pro obnovení nezbytných činností.

V rámci organizace bude existovat řízený proces pro rozvoj a udržování kontinuity činností organizace. Budou identifikovány možné příčiny přerušení činností organizace, včetně jejich pravděpodobnosti, velikosti dopadu a možných následků na bezpečnost informací. V závislosti na výsledcích hodnocení rizik bude vytvořena strategie stanovující celkový přístup k problému kontinuity činností organizace. Takto vytvořená strategie bude schválena vedením organizace a bude vytvořen a schválen plán její implementace. V procesu plánování kontinuity činností organizace bude zváženo:

a) určení a odsouhlasení všech odpovědností a postupů obnovy činností;
b) stanovení přijatelné úrovně pro ztrátu služeb nebo informací;
c) zavedení nouzových postupů tak, aby bylo možné dokončit zotavení a obnovu činností v požadovaných lhůtách. Zvláštní pozornost je třeba věnovat ohodnocení vnitřních a vnějších závislostí organizace a existujícím smlouvám;
d) provozní postupy až do obnovení činností;
e) dokumentace odsouhlasených procedur a postupů;
f) vhodné proškolení personálu o odsouhlasených havarijních procedurách a postupech, včetně krizového řízení;
g) testování a aktualizace plánů.

Plány kontinuity činností budou pravidelně testovány a aktualizovány, aby se zajistila jejich aktuálnost a efektivnost. Testy plánů kontinuity zajistí, že všichni členové týmu obnovy i ostatní dotčení pracovníci mají plány v povědomí a jsou si vědomi svých odpovědností a rolí v případě aktivace plánu.

Následující úvahy jsou kromě předešlých pokynů ve zdravotnickém prostředí důležité. Zajištění kontinuity činnosti organizace a řízení, zahrnující obnovu po haváriích, je stále více uznáváno pro zdravotnické organizace jako požadavek s rostoucí prioritou. S ohledem na přísné požadavky na dostupnost zdravotní péče by mělo být věnováno velké úsilí opatřením týkajícím se pružnosti a redundance, a to nejen pro technologii samotnou, ale také pro průřezové vzdělávání zdravotnického personálu. Plánování zajištění kontinuity činnosti organizace ve zdravotnictví je pro specialisty

v oblasti bezpečnosti informací zvláště náročné, protože jakékoliv plány je potřeba vhodně začlenit do organizačních postupů organizace pro zvládání výpadků proudů, zavádění kontroly infekcí a řešení jiných klinických nepředvídaných situací. Výskyt jakékoliv takové situace pravděpodobně povede přímo k žádosti o plán na řízení kontinuity činnosti organizace, i když často poskytne jen další podporu oproti běžně dostupné. Nicméně nedávné incidenty jako vypuknutí SARS ukázaly, že významné incidenty mohou vyvolat nedostatek pracovníků, což může vážně omezit schopnost úspěšně provozovat plány k zajištění kontinuity činnosti organizace. Zdravotnické organizace potřebují zajistit, aby jejich plánování řízení kontinuity činnosti organizace zahrnovalo plánování krizového managementu ve zdravotnictví. Zdravotnické organizace také potřebují zajistit, aby plány, které vyvíjejí, byly pravidelně testovány na „programové“ bázi. Testy obsažené v takovém programu by měly na sebe navazovat, postupujíce od testování osobních počítačů k modulárnímu testování, k syntéze pravděpodobných časů obnovy a konečně úplné zkoušky. Takový program představuje nízké riziko a je skutečným zlepšením obecné úrovně povědomí jeho uživatelské populace.

V následující tabulce jsou uvedeny potřebné zdroje, odpovědnosti a harmonogramy spojené se zaváděním opatření:

Tabulka 31 Opatření 4.2.9

Položka	Přímý náklad (odhad)	Odpovědnost	Harmonogram nasazení opatření
Identifikace možných příčin přerušení kontinuity činností organizace	1000 Kč	Koordinátor řízení kontinuity činností	Do 1 týdne
Stanovení všech odpovědností a postupů obnovy činností	2500 Kč	Koordinátor řízení kontinuity činností, bezp. manažer	Do 14 dnů
Implementace plánů kontinuity	4000 Kč	Koordinátor řízení kontinuity činností	Do 1 měsíce
Školení personálu o odsouhlasených havarijních procedurách a postupech	3000 Kč	Koordinátor řízení kontinuity činností, bezp. manažer	Ihned, 1x za půl roku
Testování a aktualizace plánů	2000 Kč	Koordinátor řízení kontinuity činností	Ihned, 1x za 3 měsíce
Celkem:	**Cca 13000 Kč**		

4.2.10 Shoda s právními požadavky

Cílem je vyvarovat se porušení norem trestního nebo občanského práva, zákonných nebo smluvních povinností a bezpečnostních požadavků.

Návrh, provoz a používání informačních systémů může být předmětem zákonných, podzákonných nebo smluvních bezpečnostních požadavků.

Specifické požadavky vyplývající ze zákona budou konzultovány s právními poradci organizace nebo jinými kvalifikovanými právníky. Legislativní požadavky na informace vzniklé v jedné zemi a přenášené do jiné země jsou různé a mění se podle jednotlivých zemí. Postup zavádění tohoto opatření bude nárazový.

Pro každý informační systém budou jednoznačně definovány, zdokumentovány a udržovány aktuální veškeré relevantní zákonné, podzákonné a smluvní požadavky a způsob jakým je organizace dodržuje.

Kromě dodržování těchto pokynů bude organizace spravovat informační souhlas subjektů péče. Pokud je to možné, měl by být tento informační souhlas subjektů péče získán před tím, než budou osobní zdravotní informace poslány e-mailem, faxovány, zmíněny v telefonické konverzaci nebo jinak zpřístupněny stranám externím ve vztahu ke zdravotnické organizaci.

Pro zajištění souladu se zákonnými, podzákonnými a smluvními požadavky při použití předmětů a aplikačního programového vybavení, které mohou být chráněny zákony na ochranu duševního vlastnictví, budou zavedeny vhodné postupy. Budou zvážena následující opatření:

a) získávání programové vybavení pouze od známých a ověřených dodavatelů;
b) udržování povědomí o pravidlech dodržování autorských práv a zdůrazňování disciplinárního řízení při jejich porušení;
c) vedení dokladů a důkazů vlastnictví licencí, instalačních disket, manuálů apod.;
d) vytvoření pravidel zajišťujících dodržování odpovídajících licenčních podmínek;
e) dodržování požadavků a podmínek u programů a informací získaných z veřejných sítí;

Důležité záznamy organizace by měly být chráněny proti ztrátě, zničení a padělání a to v souladu se zákonnými, podzákonnými a smluvními požadavky a požadavky organizace.

V následující tabulce jsou uvedeny potřebné zdroje, odpovědnosti a harmonogramy spojené se zaváděním opatření:

Tabulka 32 Opatření 4.2.10

Položka	Přímý náklad (odhad)	Odpovědnost	Harmonogram nasazení opatření
Udržování aktuálních veškerých relevantních zákonných, podzákonných a smluvních požadavků	500 Kč	Právní oddělení	Ihned, 1x za rok aktualizovat
Celkem:	**500 Kč**		

4.3 Tvorba bezpečnostních směrnic

Je důležité říci, že firma má své vnitřní směrnice, které již specifikují některé bezpečnostní aspekty. Tyto směrnice je potřeba doplnit a rozšířit o všechny důležité faktory bezpečnosti popsané ve výše uvedené bezpečnostní příručce. Konečná podoba všech těchto nově vzniklých a nově upravených interních směrnic bude předmětem schvalovacího procesu organizace.

Tvorba nových bezpečnostních směrnic je komplikovaný proces, který zahrnuje zpracování bezpečnostní příručky a sepsání všech důležitých informací o konkrétních aspektech bezpečnosti celé organizace do interních směrnic. Takto důležité dokumenty jsou v kompetenci bezpečnostního manažera firmy, který bude pro tuto činnost ve firmě teprve jmenován.

Celý tento proces vytváření bezpečnostních směrnic pomůže firmě po schválení zákona o kybernetické bezpečnosti rychleji zavést do praxe zlepšení požadované bezpečnosti informací a aktiv organizace.

4.4 Návrhy na zavádění ISMS

Jako první krok navrhuji najmout pro zavádění ISMS ve zdravotnické organizaci bezpečnostního manažera, který za tuto práci ponese odpovědnost a bude řídit celý postup zavádění. V tabulkách pod každým opatřením v bezpečnostní příručce navrhuji letmý koncept zavedení jednotlivých opatření včetně odhadu přímých nákladů, odpovědností a harmonogramu zavádění (jak kritické je dané opatření). Jsou to odhady, podle kterých se může řídit budoucí bezpečnostní manažer při zavádění ISMS do zdravotnické organizace. Z těchto odhadů mi vychází, že celý proces nasazování všech opatření podle mé bezpečnostní příručky by mohl stát až kolem 300 000 Kč, což je vzhledem k ročnímu obratu celé organizace ve výši cca 1,3 mld. nepatrná částka. Tato částka však nezahrnuje ani provoz (přezkoumávání a monitorování) ISMS ani periodická školení zaměstnanců a je nastavena pouze pro jednu pobočku, přičemž vybraná organizace má poboček další dvě desítky.

K vlastnímu nasazování navrhuji přistupovat jako k řízenému projektu. To znamená nejprve sestavit analýzu, co se všechno bude zavádět a jakým rizikům je potřeba se skutečně vyhnout. Jako další krok navrhuji sestavení projektového týmu pro nasazování ISMS. Tento tým by měl obsahovat všechny role vyjmenované v bezpečnostní příručce v kapitole 4.2.1 a navrhuji, aby byly určeny konkrétní odpovědnosti podle konceptu v tabulkách u každého opatření. Harmonogram zavádění pak hodně záleží na rychlosti komunikace celého týmu a komunikace týmu s vedením společnosti, tedy s vrcholovým managementem.

Klíčovým momentem při zavádění ISMS je pochopení motivace organizace. Proto zde uvedu ještě přínosy zavedení ISMS:

- zajištění kompatibility v oblasti bezpečnosti s ostatními organizacemi
- ujištění partnerů a zákazníků o adekvátní ochraně informací
- možnost získat mezinárodně uznávaný certifikát
- rozšíření prvků systému integrovaného managementu

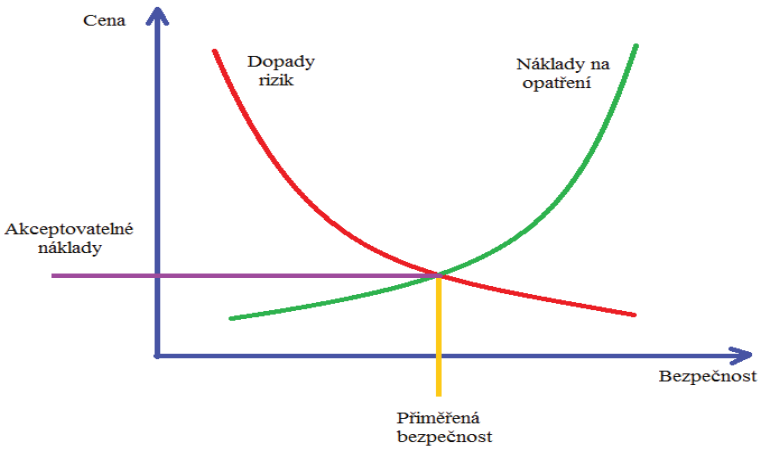
Závěr

Ve své diplomové práci jsem se zabýval informační bezpečností v oblasti zdravotnictví. Cílem mé práce bylo analyzovat problematiku systému řízení bezpečnosti informací (ISMS) ve zdravotnických organizacích a vytvořit bezpečnostní příručku pro možné nasazení ISMS v praxi na základě bezpečnostní analýzy konkrétní pobočky vybrané zdravotnické organizace.

Vybraná organizace nemá dosud vypracovanou kompletní informační bezpečnost. Potřeba vytvořit bezpečnostní příručku je v zájmu organizace i z důvodu citlivosti dat, které uchovává. Navržená bezpečnostní příručka popisuje opatření vybraná na základě hodnocení rizik organizace v souladu s požadavky na bezpečnost vyplývající z nově vznikajícího kybernetického zákona. Organizace pomocí této příručky může zavést opatření do své praxe. Viz návrh na zavádění ISMS – kapitola 4.4.

Při nasazování ISMS do jakékoliv organizace je třeba navrhnout a zpracovat tzv. *bezpečnostní politiku organizace.* V tomto dokumentu je třeba písemně vyjádřit souhlas vedení s udržováním ISMS a s přidělením zdrojů (finančních, lidských a technických) k nasazení ISMS. Dále je nezbytné definovat rozsah celého ISMS, v jakém se bude dodržovat. Tato fáze zahrnuje výběr opatření, která se aplikují. Při tomto procesu by se měl bezpečnostní manažer řídit podle principu tzv. *přiměřené bezpečnosti.* Je také možné, že se všechna opatření nezavedou najednou a proces tak nabude trvalejšího rozměru. Prvotně by se však měla zavádět opatření, která zabraňují nejkritičtějším rizikům. Velikost úsilí a investic do bezpečnosti musí odpovídat hodnotě aktiv a míře možných rizik. Princip je znázorněn na obrázku:

Obrázek 7 Přiměřená bezpečnost, Zdroj: vlastní tvorba



V praxi jsem se seznámil s provozem vybrané pobočky zdravotnické organizace, která je před celkovou rekonstrukcí. Zde jsem konzultoval praktické zkušenosti v bezpečnosti jejich provozu. Ukázalo se, že mají v této oblasti řadu problémů.

Výběr správných opatření by organizaci měla usnadnit mnou sestavená tabulka hrozeb a zranitelností (v příloze), která odkazuje na příslušné kapitoly bezpečnostní příručky s odpovídajícím opatřením ke každému riziku. Tato tabulka je optimalizována na analyzovanou pobočku. Informace z vytvořené příručky v praxi již použijí a vytvoří podmínky v projektové dokumentaci.

Hlavním přínosem této práce je její použitelnost a možnost ji začlenit do celého systému organizace, a to do všech svých poboček. Nyní záleží vše na vedení organizace, zda a jakým způsobem opatření zavede do provozu.

Jako možným budoucím směřováním vybrané organizace vidím kompletní zavedení ISMS a následnou certifikaci dle normy ČSN ISO/IEC 27001. Tento krok by jim velmi usnadnil další konání v oblasti bezpečnosti informací podle budoucích požadavků zákona o kybernetické bezpečnosti a jeho prováděcích vyhlášek.

Co se týče finančního zhodnocení mé práce, v porovnání s odhady tržních cen vypracování podobných analýz a návrhů řešení nasazování ISMS by se dalo říci, že vznikla odhadovaná úspora pro vybranou zdravotnickou organizaci cca 50000 Kč za analýzu situace HW, SW a pracovních postupů personálu na pracovišti, 80000 Kč za analýzu rizik pro konkrétní pobočku a 120000 Kč za vytvoření bezpečnostní příručky pro celou organizaci.

Domnívám se, že se můj cíl i smysl práce zcela naplnil a že bude sloužit v praxi potřebné bezpečnosti, ochraně dat a stále narůstajícím rizikům v nastávající elektronické době.

Literatura

[1] ŠALEK, Martin. Nemocnice Na Bulovce: Útok hackerů na síť Nemocnice Na Bulovce. [online]. [cit. 2014-05-22]. Dostupné z: http://bulovka.cz/aktuality/20130912-utok-hackeru-na-sit-nemocnice-na-bulovce

[2] *CSIRT - Aktuálně z bezpečnosti* [online]. [cit. 2014-05-22]. Dostupné z: http://www.csirt.cz/news/security/

[3] PRINCE, Brian. FBI Warning Highlights Healthcare's Security Infancy. [online]. [cit. 2014-05-22]. Dostupné z: http://www.darkreading.com/attacks-breaches/fbi-warning-highlights-healthcares-security-infancy/d/d-id/1234889

[4] POŽÁR, Josef. Informační bezpečnost. Plzeň: Aleš Čeněk, 2005, 309 s. Vysokoškolské učebnice (Aleš Čeněk). ISBN 80-868-9838-5.

[5] ONDRÁK, Viktor, Petr SEDLÁK a Vladimír MAZÁLEK. Problematika ISMS v manažerské informatice. Vyd. 1. Brno: CERM, 2013, 377 s. ISBN 978-80-7204-872-4.

[6] DOBDA, Luboš. Ochrana dat v informačních systémech. 1. vyd. Praha: Grada Publishing, 1998, 286 s. ISBN 80-716-9479-7.

[7] DOUCEK, Petr, Luděk NOVÁK a Vlasta SVATÁ. Řízení bezpečnosti informací. 1. vyd. Praha: Professional Publishing, 2008, 239 s. Vysokoškolské učebnice (Aleš Čeněk). ISBN 978-80-86946-88-7.

[8] Jaký bude zákon o kybernetické bezpečnosti? - Lupa.cz. [online]. [cit. 2014-05-22]. Dostupné z: http://www.lupa.cz/clanky/jaky-bude-zakon-o-kyberneticke-bezpecnosti/

[9] *Národní centrum kybernetické bezpečnosti ČR* [online]. 2013 [cit. 2014-05-22]. Dostupné z: http://www.govcert.cz/cs/

[10] *Národní bezpečnostní úřad* [online]. 2010 [cit. 2014-05-22]. Dostupné z: http://nbu.cz/cs/

[11] ČSN ISO/IEC 27799:2010 Zdravotnická informatika – Systémy řízení bezpečnosti informací ve zdravotnictví využívající ISO/IEC 27002. Český normalizační institut, 2010.

[12] Confused Xerox copiers rewrite scanned documents, expert finds. [online]. [cit. 2014-05-22]. Dostupné z: http://www.bbc.com/news/technology-23588202

[13] ČSN ISO/IEC 27001:2006 Informační technologie - Bezpečnostní techniky – Systémy managementu bezpečnosti informací – Požadavky. Český normalizační institut, 2006.

[14] ČSN ISO/IEC 27002:2005 Informační technologie – Bezpečnostní techniky – Soubor postupů pro řízení bezpečnosti informací. Český normalizační institut, 2005.

[15] ČSN ISO/IEC 27005:2013 Informační technologie - Bezpečnostní techniky - Řízení rizik bezpečnosti informací. Český normalizační institut, 2013.

Seznam příloh

Tabulka hrozeb a zranitelností ve zdravotnické organizaci

Aktivum	Hodnota	Hrozba	Zranitelnost	PI	Dopad	Riziko	Opatření
Lékařská dokumentace - elektronická	5	špatné diagnózy	Nedodržování směrnic	2	5	50	4.2.5.1
		ztráta dat	porucha zálohování, viry, nasazení destruktivních programů	1	5	25	4.2.5.5 4.2.5.4
		krádež dat	špatné zabezpečení IS	1	5	25	4.2.5.6 a 4.2.5.3
		zneužití dat	únik informací	3	5	75	4.2.6.6
Lékařská dokumentace - papírová	4	špatné diagnózy	Nedodržování směrnic	2	5	37	4.2.5.1
		ztráta dat	oheň, voda	1	3	11	4.2.4.1
		krádež dat	nezabezpečení archivu	1	4	15	4.2.4.1
		zneužití dat	únik informací	3	5	55	4.2.6.3
Osobní údaje personálu	3	krádež dat	nezabezpečení dokumentů	1	4	13	4.2.4.1
		zneužití dat	špionáž, platy	3	4	40	4.2.6.3
Faktury zdravotním pojišťovnám	3	poškození dat	chybné zpracování administrátorem	3	4	36	4.2.5.1
		ztráta dat	poškození datového úložiště	2	2	12	4.2.5.5
		krádež dat	špionáž na síti	1	3	9	4.2.6.4
Interní směrnice	4	neznalost personálu	chybné prac. postupy	4	4	59	4.2.5.1
		nedbalost personálu	zjednodušování úkolů	3	4	44	4.2.5.1
		krádež dat	únik informací	2	4	29	4.2.2.2
Docházkový systém	4	nedbalost personálu	označení příchod,odchod	3	2	24	4.2.4.1
		podvod personálem	pozdější odchod	3	3	36	4.2.3.2
		nefunkčnost	neoznačení přítomnosti	3	2	24	4.2.5.2
Zdravotnický software	5	chyba v zabezpečení	možnost napadení hackery	1	5	25	4.2.7.1
		nedostatečná funkčnost	zdržování personálu	4	3	60	4.2.5.3
		nedostatečná školení	nevyužití funkcí programu	4	3	60	4.2.3.2
		lidské neúmyslné	neukládání práce	2	2	20	4.2.3.2
			neodhlášení se	2	4	40	4.2.3.2
		lidský úmyslný - vnitřní	zneužití služeb - souběh praxí	2	3	30	4.2.3.1
Technický software	4	chyba v zabezpečení	neaktualizovaný OFFICE - viry	3	3	33	4.2.5.4
		nedostatečná funkčnost	zdržování personálu	3	2	22	4.2.5.3
		nedostatečná školení	nevyužití funkcí programu	3	3	33	4.2.3.2
Operační systémy	5	chyba v zabezpečení	neaktualizovaný OS - hackeři	2	4	40	4.2.5.3
			zavedení destruktivních nebo sledovacích programů	1	5	25	4.2.5.4
		lidské neúmyslné	neodhlášení se	3	3	45	4.2.3.2
			stahování nebezpečných SW	2	4	40	4.2.5.4
Server	5	přírodní a fyzické	živelné nebezpečí zvenku	2	4	40	4.2.4.1
			vyplavení zařízení	3	4	60	4.2.4.1
			elektřina - poskytovatel	2	4	40	4.2.4.2
			elektřina - vnitřní	3	4	60	4.2.4.2
		technické a technologické	poruchy, viry	2	4	40	4.2.5.2
		lidské neúmyslné	mechanické poškození, viry	3	4	60	4.2.5.4
		lidské úmyslné-vnitřní	viry, nasazení odposlechu	1	5	25	4.2.3.1
		lidské úmyslné-vnější	viry,špionáž,hacker.útoky- DDOS, BOTNET…	3	5	75	4.2.5.6
Koncové stanice - 7 PC	4	přírodní a fyzické	živelné nebezpečí zvenku	2	3	24	4.2.4.1
			vyplavení zařízení	1	3	12	4.2.4.1
			elektřina - poskytovatel	2	3	24	4.2.4.2
			elektřina - vnitřní	3	3	36	4.2.4.2
		technické a technologické	poruchy, viry	3	3	36	4.2.5.2
		lidské neúmyslné	mechanické poškození, tekutiny	3	3	36	4.2.4.2
			krádež PC	2	3	24	4.2.2.1
		lidské úmyslné-vnitřní	neoprávněné použití PC	3	4	48	4.2.4.1
			rozbití PC	2	3	24	4.2.2.1
		lidské úmyslné-vnější	viry,špionáž,hacker.útoky	2	5	40	4.2.5.4 a 4.2.5.6
Periferie - tiskárny, čtečky pac.karet, scanner	2	přírodní a fyzické	živelné nebezpečí zvenku	2	3	14	4.2.4.1
			vyplavení zařízení	1	3	7	4.2.4.1
			elektřina - poskytovatel	2	3	14	4.2.4.2
			elektřina - vnitřní	3	3	21	4.2.4.2
		technické a technologické	poruchy periferií	3	3	21	4.2.5.2
		lidské neúmyslné	mechanické poškození, tekutiny	4	3	28	4.2.4.2
		lidské úmyslné-vnitřní	mechanické poškození, krádež	2	3	14	4.2.2.1
		lidské úmyslné-vnější	krádeže	2	3	14	4.2.4.1
Síťové prvky	5	přírodní a fyzické	živelné nebezpečí zvenku	2	4	40	4.2.4.1
			vyplavení zařízení	1	4	20	4.2.4.1
			elektřina - poskytovatel	2	4	40	4.2.4.2
			elektřina - vnitřní	3	4	60	4.2.4.2
		technické a technologické	poruchy síťových prvků	3	4	60	4.2.5.2
		lidské neúmyslné	přepojení kabelů uklízečkou	3	3	45	4.2.4.2
			omezení funkčnosti aktivních prvků	3	3	45	4.2.4.2
		lidské úmyslné-vnitřní	mechanické poškození, krádež	2	4	40	4.2.4.1
		lidské úmyslné-vnější	zneužití WiFi	3	5	75	4.2.6.7
Komunikační trasy	5	přírodní a fyzické	tzv. blackout	1	5	25	4.2.5.6
		technické a technologické	poruchy sítí	1	4	20	4.2.5.6
		lidské neúmyslné	přerušení	2	4	40	4.2.5.6
		lidské úmyslné-vnější	přerušení,odposlech	3	5	75	4.2.5.6
Základní služby (světlo,voda,teplo klimatizace,zabezpečení pracoviště)	3	přírodní a fyzické	nedostatečné zabezpečení proti živelným pohromám	2	4	21	4.2.4.1
		technické a technologické	el.rozvaděče vně objektu,	4	4	43	4.2.4.1
			staré rozvody vody,el.proudu	3	4	32	4.2.4.2
			nevyhovující pracovní prostředí - světlo, teplo, ergonomie, rozmístění pracoviště	4	3	32	4.2.4.2
		lidské neúmyslné	zapomenutí zabezpečení objektu	3	5	40	4.2.2.1
		lidské úmyslné-vnitřní	sabotáž bezpečnosti	2	5	27	4.2.3.1
		lidské úmyslné-vnější	volný přístup do rozvaděčů	1	4	11	4.2.4.1
			zničení pracoviště	1	4	11	4.2.4.1
			krádež zařízení	2	4	21	4.2.4.1

HLÁŠENÍ KYBERNETICKÉHO BEZPEČNOSTNÍHO INCIDENTU	
MÍRA OCHRANY INFORMACE	
Úroveň ochrany	
	Osobní – seznam příjemců Omezená distribuce Neomezeno
KONTAKTNÍ ÚDAJE	
Orgán a osoba uvedená v § 3 písm. c) a e) zákona	
Email	
Telefon	
DETAILY INCIDENTU	
Datum a čas zjištění	
Časová zóna	
Kategorie incidentu	Kategorie III – velmi závažný kybernetický bezpečnostní incident Kategorie II – závažný kybernetický bezpečnostní incident Kategorie I – méně závažný kybernetický bezpečnostní incident
Typ incidentu	Kybernetický bezpečnostní incident způsobený kybernetickým útokem nebo jinou událostí vedoucí k průniku do systému nebo k omezení dostupnosti služeb. Kybernetický bezpečnostní incident způsobený škodlivým softwarem nebo kódem. Kybernetický bezpečnostní incident způsobený kompromitací technických opatření. Kybernetický bezpečnostní incident způsobený porušením organizačních opatření. Ostatní kybernetické bezpečnostní incidenty způsobené kybernetickým útokem. Kybernetický bezpečnostní incident způsobující narušení důvěrnosti primárních aktiv. Kybernetický bezpečnostní incident způsobující narušení integrity primárních aktiv. Kybernetický bezpečnostní incident způsobující narušení dostupnosti primárních aktiv. Kybernetický bezpečnostní incident způsobující kombinaci dopadů uvedených shora.
Současný stav	Probíhá Pod kontrolou Obnoveno Neznámý
Počet zasažených systémů (odhad)	
Popis incidentu	
SYSTÉMOVÉ DETAILY	
Host nebo IP	
Funkce hosta (DNS server, stanice atd.)	
Pokračování	Iniciační oznámení CERTu Pokračování dříve oznámených